DATA TRANSFERRING SYSTEM, DATA TRANSFERRING DEVICE, DATA RECORDING DEVICE, DATA MANAGING METHOD AND IDENTIFIER GENERATING METHOD

Publication number: JP2002366441 (A)
Publication date: 2002-12-20
Inventor(s): ABE MIKI; HOSOI TAKASHI; MATSUDA HIROMI; TANAKA YOSHIO
Applicant(s): SONY CORP
Classification:
- international: *G06F12/14; G06F12/00; G06F21/00; G06F21/24; G09C1/00; G11B20/00; G11B27/034; G11B27/10; H04L9/08; H04L29/06; H04N7/173;* G11B20/10; G11B20/12; G06F12/14; G06F12/00; G06F21/00; G09C1/00; G11B20/00; G11B27/031; G11B27/10; H04L9/08; H04L29/06; H04N7/173; G11B20/10; G11B20/12; (IPC1-7): G06F12/14; G06F12/00; G09C1/00; H04L9/08; H04N7/173
- European: H04L29/06S4B; G06F21/00N7D; G11B20/00P; G11B27/034; G11B27/10A1
Application number: JP20010178512 20010613
Priority number(s): JP20010178512 20010613

Also published as:

JP3778009 (B2)
US2004015713 (A1)
US7350238 (B2)
RU2284591 (C2)
WO02103529 (A1)
more >>

Abstract of JP **2002366441** (A)

PROBLEM TO BE SOLVED: To realize the proper management and operating efficiency of contents transfer. SOLUTION: A data transferring device side (primary recording medium side) manages the transfer right of respective stored contents data, and also manages the transfer right of contents data transferred to a data recording device (secondary recording medium side) in a state that table data in which a first contents identifier corresponding to the contents data is made correspond to a second contents identifier transmitted from the recording device side are generated.; That is, even when it is not possible to record the contents identifier (contents ID) at the secondary recording medium side, it is possible to identify the contents data on the secondary recording medium by using the contents ID (second contents identifier) generated at the secondary recording medium side, and to make this correspond to the contents ID (first contents identifier) at the primary recording medium side.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－366441
（P2002－366441Ａ）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
12/00	５３７	12/00	５３７Ｈ	５Ｂ０８２
	５４５		５４５Ｍ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　7/173	６３０	

審査請求　未請求　請求項の数25　ＯＬ　（全 49 頁）　最終頁に続く

(21)出願番号　特願2001－178512(P2001－178512)
(22)出願日　平成13年６月13日(2001.6.13)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　阿部　三樹
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　細井　隆史
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100086841
弁理士　脇　篤夫　（外１名）

最終頁に続く

(54)【発明の名称】　データ転送システム、データ転送装置、データ記録装置、データ管理方法、識別子生成方法

(57)【要約】
【課題】　コンテンツ転送の適切な管理及び動作の効率化。
【解決手段】　データ転送装置側（一次記録媒体側）では、格納されている各コンテンツデータについての転送権利を管理するとともに、データ記録装置（二次記録媒体側）に対して転送したコンテンツデータについては、そのコンテンツデータに対応する第１のコンテンツ識別子とデータ記録装置側から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する。つまり二次記録媒体側でコンテンツ識別子（コンテンツＩＤ）を記録できない場合でも、二次記録媒体側で発生させるコンテンツＩＤ（第２のコンテンツ識別子）を用いて二次記録媒体上のコンテンツデータを識別でき、しかもそれが一次記録媒体側のコンテンツＩＤ（第１のコンテンツ識別子）と対応づけられるようにする。

コンテンツID　対応テーブル

PCアプリケーションによるコンテンツID1	二次記録媒体制御部によるコンテンツID1
PCアプリケーションによるコンテンツID2	二次記録媒体制御部によるコンテンツID2
PCアプリケーションによるコンテンツID3	二次記録媒体制御部によるコンテンツID3

【特許請求の範囲】
【請求項１】　データ転送装置と、データ記録装置とから成るデータ転送システムにおいて、
上記データ転送装置は、
一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、
暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第１のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、
上記データ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、
上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して転送したコンテンツデータについては、該コンテンツデータに対応する上記第１のコンテンツ識別子と上記データ記録装置側から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、
を備え、
上記データ記録装置は、
上記データ転送装置との間で、コンテンツデータの受信を含む各種データ通信を行う通信手段と
二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、
上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態に復号する復号手段と、
上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、
非暗号化状態のコンテンツデータから上記第２のコンテンツ識別子を生成する識別子生成手段と、
上記識別子生成手段で生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、
を備えたことを特徴とするデータ転送システム。
【請求項２】　上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理することを特徴とする請求項１に記載のデータ転送システム。
【請求項３】　上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第２のコンテンツ識別子を要求し、送信されてきた第２のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項１に記載のデータ転送システム。
【請求項４】　上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理により上記第２のコンテンツ識別子を生成することを特徴とする請求項１に記載のデータ転送システム。
【請求項５】　上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとされることを特徴とする請求項４に記載のデータ転送システム。
【請求項６】　上記データ転送装置からコンテンツデータが転送されてくる際に、
上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記第２のコンテンツ識別子を生成し、
上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項４に記載のデータ転送システム。
【請求項７】　コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合に、
上記二次記録媒体ドライブ手段は、
上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、
上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第２のコンテンツ識別子が要求された際には、
上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記第２のコンテンツ識別子を生成し、
上記識別子送信制御手段は、生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項４に記載のデータ転送システム。
【請求項８】　コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合に、
上記二次記録媒体ドライブ手段は、
上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、
上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記第２のコンテンツ識別子を生成して記憶手段に記憶させておき、
上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第２のコンテンツ識別子が要求された際には、
上記識別子送信制御手段は、上記記憶手段に記憶されて

いる上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項４に記載のデータ転送システム。

【請求項９】　一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、
暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第１のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、
外部のデータ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、
上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して或るコンテンツデータを転送した際には、該コンテンツデータに対応する上記第１のコンテンツ識別子と上記データ記録装置側から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、
を備えたことを特徴とするデータ転送装置。

【請求項１０】　上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理することを特徴とする請求項９に記載のデータ転送装置。

【請求項１１】　上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第２のコンテンツ識別子を要求し、送信されてきた第２のコンテンツ識別子と上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項９に記載のデータ転送装置。

【請求項１２】　外部のデータ転送装置との間で、コンテンツデータの受信を含む各種データ通信を行う通信手段と二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態に復号する復号手段と、
上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、
非暗号化状態のコンテンツデータからコンテンツ識別子を生成する識別子生成手段と、
上記識別子生成手段で生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、
を備えたことを特徴とするデータ記録装置。

【請求項１３】　上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理により上記コンテンツ識別子を生成することを特徴とする請求項１２に記載のデータ記録装置。

【請求項１４】　上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとされることを特徴とする請求項１３に記載のデータ記録装置。

【請求項１５】　上記データ転送装置からコンテンツデータが転送されてくる際に、
上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記コンテンツ識別子を生成し、
上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項１３に記載のデータ記録装置。

【請求項１６】　コンテンツデータが記録された上記二次記録媒体が装填されている場合に、
上記二次記録媒体ドライブ手段は、
上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、
上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記コンテンツ識別子が要求された際には、
上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記コンテンツ識別子を生成し、
上記識別子送信制御手段は、生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項１３に記載のデータ記録装置。

【請求項１７】　コンテンツデータが記録された上記二次記録媒体が装填されている場合に、
上記二次記録媒体ドライブ手段は、
上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、
上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記コンテンツ識別子を生成して記憶手段に記憶させておき、
上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記コンテンツ識別子が要求された際には、
上記識別子送信制御手段は、上記記憶手段に記憶されている上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項１３

に記載のデータ記録装置。

【請求項１８】　暗号化されて一次記録媒体に記録されたコンテンツデータについての、二次記録媒体への転送権利を管理するデータ管理方法において、

上記各コンテンツデータについて生成した第１のコンテンツ識別子にそれぞれ対応させて、各コンテンツデータの転送権利を管理すると共に、

二次記録媒体へ転送したコンテンツデータについては、該コンテンツデータに対応する上記第１のコンテンツ識別子と上記二次記録媒体側機器から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理することを特徴とするデータ管理方法。

【請求項１９】　各コンテンツデータについての上記転送権利として、外部の二次記録媒体に対する転送許可回数を管理することを特徴とする請求項１８に記載のデータ管理方法。

【請求項２０】　二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、二次記録媒体側機器に対して、当該コンテンツデータについての上記第２のコンテンツ識別子を要求し、送信されてきた第２のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項１８に記載のデータ管理方法。

【請求項２１】　コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理によりコンテンツ識別子を生成することを特徴とする識別子生成方法。

【請求項２２】　上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとされることを特徴とする請求項２１に記載の識別子生成方法。

【請求項２３】　暗号化されたコンテンツデータが受信され、非暗号化状態に復号されて記録媒体に記録される場合に、

復号されたコンテンツデータが上記記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理によりコンテンツ識別子を生成することを特徴とする請求項２１に記載の識別子生成方法。

【請求項２４】　記録媒体に記録されている各コンテンツデータについて、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生して記憶しておき、

上記外部機器から上記記録媒体に記録されているコンテンツデータについてのコンテンツ識別子が要求された際に、上記記憶したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成することを特徴とする請求項２１に記載の識別子生成方法。

【請求項２５】　記録媒体に記録されている各コンテンツデータについて、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生し、再生したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成して記憶しておくことを特徴とする請求項２１に記載の識別子生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音楽等のコンテンツデータの転送／記録に好適な、データ転送システム、データ転送装置、データ記録装置、データ管理方法、識別子生成方法に関するものである。

【０００２】

【従来の技術】例えばパーソナルコンピュータのＨＤＤ（ハードディスクドライブ）を一次記録媒体として扱って音楽等のコンテンツデータを格納するとともに、格納したコンテンツデータを転送して他の記録媒体（二次記録媒体）に記録し、その二次記録媒体側で音楽等の再生を楽しむという使用形態がある。なおコンテンツデータとは、例えば音楽データ、映像データ、ゲームデータ、コンピュータソフトウエアなどの配信／転送／使用の目的となる主たるデータのことである。

【０００３】この場合、ＨＤＤには、ＣＤ－ＤＡ（Compact Disc Digital Audio）やＤＶＤ（Digital Versatile Disc）などのパッケージメディアから再生された音楽等のコンテンツデータが蓄積されたり、或いはパーソナルコンピュータが接続された通信ネットワークを介して外部の音楽サーバ等からダウンロードされたコンテンツデータが蓄積される。そしてユーザーは、パーソナルコンピュータに二次記録媒体の記録装置を接続して、ＨＤＤに蓄積されたコンテンツデータを二次記録媒体にコピー（複製）又はムーブ（移動）し、当該二次記録媒体に対応する再生装置で音楽等のコンテンツデータを再生させる。

【０００４】二次記録媒体としては、例えばフラッシュメモリ等の半導体メモリを利用したメモリカードや、光磁気ディスクとしてのミニディスク、或いはＣＤ－Ｒ（ＣＤ Recordable）、ＣＤ－ＲＷ（ＣＤ Rewitable）、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷなどが考えられる。二次記録媒体に対応する記録装置、再生装置として、これらのメディア（記録媒体）に対応するレコーダ／プレーヤは、広く普及しており、据置型の記録再生装置や、ポータブルタイプの記録再生装置などとして多様に存在し、各ユーザーはそれぞれ自分の好みや所有する機器に合わせて、コンテンツデータの記録／再生を行うものとなる。

【０００５】なお、例えばこのようなコンテンツデータの使用形態を考えるときは、コンテンツデータについて

の著作権保護を考慮しなければならない。例えばユーザーがコンテンツデータの配信サービスを利用したり、パッケージメディアの購入を行うなどして、HDDにコンテンツデータを蓄積した後、そのコンテンツデータを無制限に二次記録媒体にコピー可能とすると、著作権者の正当な保護がはかれない事態が生ずる。このためデジタルデータとしてのコンテンツデータの扱い上で著作権保護を維持できるようにする様々な技術やデータ処理上の取り決めが提案されているが、その1つにSDMI（SECURE DIGITAL MUSIC INITIATIVE）という規格がある。このSDMIで策定されたデータパスについては後述するが、例えば一次記録媒体としてのHDDを備えたパーソナルコンピュータに蓄積されたコンテンツ、例えばネットワークを介して外部サーバから配信されたコンテンツデータ（以下、ネットワークコンテンツ）や、例えばパーソナルコンピュータに装備されているCD－ROMドライブ等のディスクドライブ装置、或いはパーソナルコンピュータと接続されたディスクドライブ装置において再生されるCD－DA、DVD等のパッケージメディアから読み出されたコンテンツデータ（以下、ディスクコンテンツ）について、二次記録媒体への転送／記録が、著作権保護と一般ユーザーの利益（私的複製の権利）を勘案したうえで、適切に行われるようにされている。

【０００６】ところで、HDD等の一次記録媒体からミニディスクやメモリカード等の二次記録媒体へコンテンツデータを転送してコピーする場合においては、上記のように著作権保護や私的複製の権利の双方を満たすための工夫が施されている。

【０００７】即ち上記SDMI対応の二次記録媒体に対する転送については次のようになっている。SDMI対応の二次記録媒体とは、例えばフラッシュメモリ等の半導体メモリを利用したSDMI対応のメモリカードなどが想定され、この二次記録媒体にはコンテンツが暗号化された状態で記録される。例えばHDDなどの一次記録媒体では、SDMI方式のコンテンツの場合は暗号化が施されて蓄積されるが、従って、その暗号化状態のまま二次記録媒体にコピーされるものとなる。もちろん二次記録媒体に対する再生機器では、暗号解読機能が備えられており、従って暗号化状態でコピーされたコンテンツデータを再生させることができる。

【０００８】またSDMI対応の二次記録媒体では各コンテンツデータについての識別子となるコンテンツＩＤを記録する領域がフォーマット上、用意されている。コンテンツＩＤは、一次記録媒体側の機器において一次記録媒体（HDD）に蓄積された各コンテンツデータについて生成し、コンテンツデータとともに格納しておくものであるが、コンテンツデータを二次記録媒体にコピーする場合には、そのコンテンツデータについてのコンテンツＩＤも、二次記録媒体に記録されるものとなる。

【０００９】コンテンツＩＤは、一次記録媒体側と二次記録媒体側でのコンテンツ権利管理に用いられる。ここでいうコンテンツ権利とは、一次記録媒体側については、二次記録媒体への転送権（二次記録媒体にコピーさせる権利）であり、二次記録媒体側については、コピーしたコンテンツデータの再生権となる。なお、以下、一次記録媒体から二次記録媒体へのコンテンツデータの転送（権利譲渡）を「チェックアウト」といい、また二次記録媒体から一次記録媒体へのコンテンツデータの返却（実際には権利の返却）を「チェックイン」と呼ぶ。

【００１０】SDMI方式では、チェックアウト、チェックインに関しては、転送の取り扱いルール（Usage Rule）が決められる。一例としては、1つのコンテンツデータについて、一次記録媒体から二次記録媒体へのチェックアウトは3回許される（上記転送権は「3回」となる）。チェックアウトが行われると、権利が二次記録媒体側へ譲渡されることになり、つまり一次記録媒体側では、そのコンテンツデータの転送権の残りは2回となる。一方、二次記録媒体側では再生権を得ることになる。また、二次記録媒体から一次記録媒体にチェックインを行うと、権利が返却されるものとなる。つまり、二次記録媒体側では再生権を失い、一次記録媒体側では転送権が1つ復活される。

【００１１】このようなチェックアウト／チェックインの管理は、各コンテンツデータ毎にコンテンツＩＤを用いて行われる。そしてチェックアウトの際には、コンテンツデータ及びコンテンツＩＤが二次記録媒体側に記録されることで、二次記録媒体側ではコンテンツデータの再生が可能となる（再生権を得る）。一次記録媒体では、コンテンツＩＤを1つ譲渡したとみなして、Usage Ruleによる転送権を1つ減少させる。またチェックインの際には、実際にはコンテンツデータの返却転送は行われず、二次記録媒体でコンテンツデータを消去し、一次記録媒体側ではコンテンツＩＤが返却されたとして、Usage Ruleによる転送権を1つ増加させる。二次記録媒体側では再生権を失うことになる。

【００１２】このようにSDMI対応の二次記録媒体については、コンテンツデータが暗号化状態でコピー記録されること、及びチェックアウト、チェックインに応じてコンテンツの権利が管理されることで、無制限なコピーを防止して著作権保護をはかり、又一方でユーザーの私的複製権を確保している。

【００１３】なお、例えば外部サーバから一次記録媒体としてのHDDにダウンロードされて格納されるコンテンツデータは、コンテンツキーＣＫで暗号化されたものである。本明細書における説明上、一次記録媒体であるHDDには、ＡＴＲＡＣ３方式（もちろん他の圧縮方式でもよいが）で圧縮されたコンテンツデータ「Ａ３Ｄ」がコンテンツキーＣＫで暗号化されて格納されているとする。

【００１４】そして、本明細書では説明上、鍵（キー）ｘで暗号化されたデータｙを、
Ｅ（ｘ，ｙ）
と表す。またその暗号化データＥ（ｘ，ｙ）について、鍵ｘにより暗号化を復号したデータを、
Ｄ｛ｘ，Ｅ（ｘ，ｙ）｝
と表すことよする。従って、例えば上記のようにＡＴＲＡＣ３方式の圧縮データを「Ａ３Ｄ」とすると、コンテンツキーＣＫで暗号化されたコンテンツデータ「Ａ３Ｄ」は、
Ｅ（ＣＫ，Ａ３Ｄ）
となる。またＥ（ＣＫ，Ａ３Ｄ）が、鍵ＣＫで復号されたデータは、
Ｄ｛ＣＫ，Ｅ（ＣＫ，Ａ３Ｄ）｝
と表わせられる。

【００１５】また一次記録媒体であるＨＤＤには、暗号化コンテンツデータＥ（ＣＫ，Ａ３Ｄ）とともに、ルートキーＫＲで暗号化された状態のコンテンツキーＣＫ、つまり、Ｅ（ＫＲ，ＣＫ）も格納される。例えば外部サーバから暗号化コンテンツデータＥ（ＣＫ，Ａ３Ｄ）とともに、暗号化コンテンツキーＥ（ＫＲ，ＣＫ）がダウンロードされる。この場合、一次記録媒体であるＨＤＤから二次記録媒体にコンテンツデータを転送する場合、暗号化コンテンツデータＥ（ＣＫ，Ａ３Ｄ）と暗号化コンテンツキーＥ（ＫＲ，ＣＫ）を送信すればよい。二次記録媒体側機器では、ルートキーＫＲを保持していることで、ルートキーＫＲを用いてコンテンツキーＣＫを復号し、さらに復号したコンテンツキーＣＫを用いて暗号化コンテンツデータを復号できるものとなる。ただしルートキーＫＲは、著作権者側の意志や各種事情によって変更されるものであり、コンテンツデータ毎に異なるルートキーＫＲを設定することもできる。また具体例については後述するが、ルートキーＫＲの処理によってコンテンツ配信先を限定できる機能を有する。このため、ＥＫＢ（Enabling Key Block：有効化キーブロック）と呼ばれるデータが配信されることもあり、コンテンツデータが転送される正規の端末では、ＥＫＢによってルートキーを確認できるようにした方式も採られている。つまりＥＫＢも上記暗号化コンテンツデータや暗号化コンテンツキーとともにサーバから配信されＨＤＤに格納される。

【００１６】
【発明が解決しようとする課題】ここで、現在広く普及しているミニディスク（光磁気ディスク）を二次記録媒体として用いることを考える。例えばＳＤＭＩ対応のミニディスク記録装置を考える場合、そのミニディスク記録装置は、チェックアウトされたコンテンツデータについて、暗号化されたままのＥ（ＣＫ，Ａ３Ｄ）の状態でミニディスクに記録するものとされる。そして再生時にはＳＤＭＩ対応のミニディスク再生装置が、Ｄ｛ＣＫ，Ｅ（ＣＫ，Ａ３Ｄ）｝＝Ａ３Ｄとして暗号解読されたＡＴＲＡＣ３データ（Ａ３Ｄ）を得たうえで、所定のデコード処理を行って音楽等の再生出力を行うことになる。

【００１７】一方、一般に普及しているミニディスクシステムでは、ミニディスクに暗号化データを記録するものではない。当然、ミニディスク再生装置としては暗号解読の機能はない。従って、ＳＤＭＩ対応のミニディスク記録装置でコンテンツデータをミニディスクに記録したとしても、そのミニディスクに記録されたコンテンツデータを、ＳＤＭＩ対応でない多くのミニディスクプレーヤでは再生できないものとなる。つまり再生互換性が得られない。これは、一般ユーザーが購入したＳＤＭＩコンテンツの適正な利用を制限するものとなり、一般ユーザに対するＳＤＭＩコンテンツ提供サービスの価値や満足度を大きく低下させることがある。

【００１８】このような点を考慮すると、ＳＤＭＩコンテンツを二次記録媒体にコピー記録する際に、暗号化を解いた状態で、例えばＳＤＭＩに対応していないミニディスク記録装置に転送し、そのまま暗号化されていない状態でミニディスク等の二次記録媒体に記録できるようにすることが考えられる。しかしながらそのようなコピーを可能とすることは、コンテンツデータのコピーを容易に可能とすることになる。これは違法なコピーが可能となる余地を残してしまうことにもなり、ＳＤＭＩの本来の目的である著作権保護が実現できないおそれがある。

【００１９】そこでコンテンツデータ転送の一手法として、次のような転送方式を本出願人は先に提案している。即ち、コンテンツデータ転送の際には、データ転送装置（一次記録媒体側機器）が転送先となるデータ記録装置（二次記録媒体側機器）の認証を行い、認証ＯＫとなること、及びコンテンツ提供者側（著作権者等）の許諾があることを条件として暗号化データを転送許可する。そしてコンテンツデータは暗号化状態で伝送路上を転送するが、二次記録媒体へは暗号化を解いて記録するものである。また、チェックアウト、チェックインについての権利管理も行われる。これによって、非暗号化状態でのコピー記録を許容してユーザーの便宜を図ると共に、著作権保護機能が失われないようにする。

【００２０】しかしながらこのような転送方式については、以下のような問題がある。従来より普及しているミニディスク等のメディアを二次記録媒体として、ＳＤＭＩコンテンツのチェックアウト／チェックインを行おうとする場合、ミニディスク側にコンテンツＩＤを記録できないという事情がある。つまりミニディスク上ではコンテンツＩＤを記録する領域は用意されていないし、また既に普及しているミニディスクレコーダではコンテンツＩＤを管理する機能がない。例えばミニディスクの管理領域（Ｕ－ＴＯＣ）などにコンテンツＩＤを記録する領域を新たに設定することはできても、従前のミニディ

スクレコーダで記録や編集が行われてU－TOCが更新されてしまえば、コンテンツＩＤは失われてしまう。つまり従前の機器との互換性を得てユーザーの便宜を図ることで、ミニディスク側でコンテンツＩＤを管理できない。そしてコンテンツＩＤが管理できないため、例えばチェックイン管理ができないものとなる。

【００２１】一方、ミニディスク等の二次記録媒体側で例えばコンテンツデータそのものから各コンテンツデータの識別子となるコンテンツＩＤを生成することは可能である。しかしながらコンテンツＩＤの生成のためにはディスクをシークしてコンテンツデータの一部の読出などが必要であり、処理に時間がかかるという難点があると共に、そのようにして二次記録媒体側でコンテンツＩＤを生成しても、一次記録媒体側のコンテンツＩＤと一致しないため、結局管理不能となる。

【００２２】

【課題を解決するための手段】本発明はこのような事情に応じて、一次記録媒体と、非暗号化状態でコンテンツデータを記録する二次記録媒体との間でのコンテンツデータの転送管理を適切に行うことができるようにし、また処理の効率化を実現することを目的とする。

【００２３】このため本発明では、データ転送装置と、データ記録装置とから成るデータ転送システムを提供する

【００２４】そして本発明のデータ転送装置は、一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第１のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、上記データ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して転送したコンテンツデータについては、該コンテンツデータに対応する上記第１のコンテンツ識別子と上記データ記録装置側から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、を備えるものとする。

【００２５】また、上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理する。また上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第２のコンテンツ識別子を要求し、送信されてきた第２のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新する。

【００２６】また本発明のデータ記録装置は、上記データ転送装置との間で、コンテンツデータの受信を含む各種データ通信を行う通信手段と二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態に復号する復号手段と、上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、非暗号化状態のコンテンツデータから上記第２のコンテンツ識別子を生成する識別子生成手段と、上記識別子生成手段で生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、を備えるようにする。

【００２７】また上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理により上記第２のコンテンツ識別子を生成する。この場合、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとする。

【００２８】また、上記データ転送装置からコンテンツデータが転送されてくる際に、上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記第２のコンテンツ識別子を生成し、上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合には、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第２のコンテンツ識別子が要求された際には、上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記第２のコンテンツ識別子を生成し、上記識別子送信制御手段は、生成された上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。又は、コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合には、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記第２のコンテンツ識別子を生成して記憶手段に記憶させておき、上記データ転送装

置から上記二次記録媒体に記録されているコンテンツデータについての上記第２のコンテンツ識別子が要求された際には、上記識別子送信制御手段は、上記記憶手段に記憶されている上記第２のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。

【００２９】本発明のデータ管理方法は、暗号化されて一次記録媒体に記録されたコンテンツデータについての、二次記録媒体への転送権利を管理するデータ管理方法として、上記各コンテンツデータについて生成した第１のコンテンツ識別子にそれぞれ対応させて、各コンテンツデータの転送権利を管理すると共に、二次記録媒体へ転送したコンテンツデータについては、該コンテンツデータに対応する上記第１のコンテンツ識別子と上記二次記録媒体側機器から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する。この場合、各コンテンツデータについての上記転送権利として、外部の二次記録媒体に対する転送許可回数を管理する。また二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、二次記録媒体側機器に対して、当該コンテンツデータについての上記第２のコンテンツ識別子を要求し、送信されてきた第２のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新する。

【００３０】本発明の識別子生成方法は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理によりコンテンツ識別子を生成する。この場合、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとする。また暗号化されたコンテンツデータが受信され、非暗号化状態に復号されて記録媒体に記録される場合に、復号されたコンテンツデータが上記記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理によりコンテンツ識別子を生成する。また記録媒体に記録されている各コンテンツデータについては、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生して記憶しておき、上記外部機器から上記記録媒体に記録されているコンテンツデータについてのコンテンツ識別子が要求された際に、上記記憶したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成する。或いは、記録媒体に記録されている各コンテンツデータについては、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生し、再生したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成して記憶しておく。

【００３１】以上のような本発明によれば、データ転送装置とデータ記録装置との間のコンテンツデータのチェックアウト／チェックインに応じた権利管理を、第１，第２のコンテンツ識別子（コンテンツＩＤ）を用いて適正に行うことができる。またデータ記録装置側での第２のコンテンツ識別子の生成も効率化される。

【００３２】

【発明の実施の形態】以下、本発明の実施の形態を次の順序で説明する。

１．暗号化キーのツリー構造及びＥＫＢ
２．システム構成
３．ＳＤＭＩコンテンツのデータパス
４．データ転送装置の構成例（一次記録媒体側機器／ＰＣ）
５．データ記録装置の構成例（二次記録媒体側機器／記録再生装置）
６．ミニディスクの管理方式
７．認証処理
８．コンテンツ暗号化方式
９．各種コマンド
１０．コンテンツのチェックアウト／チェックイン
１１．コンテンツＩＤの生成及び管理方式
１２．チェックアウト時及びチェックイン前のコンテンツＩＤの生成処理
１３．コンテンツ書込制御フラグ
１４．課金情報処理

【００３３】１．暗号化キーのツリー構造及びＥＫＢ

まず実施の形態の転送システムの具体的な説明に先立って、コンテンツ配信に用いられる暗号化方式キーの構造を説明する。このため図１、図２、図３を用いて、コンテンツ配信側からコンテンツ受信側の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵（キー）の保有構成およびデータ配信構成を説明していく。

【００３４】図１は、暗号化キーのツリー構造を示しており、図１の最下段に示すナンバＤＶ０～ＤＶ１５がコンテンツ受信側となる個々のデバイスである。すなわち図示する階層ツリー構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

【００３５】各デバイスＤＶ０～ＤＶ１５は、製造時あるいは出荷時、あるいはその後において、図１に示す階層ツリー構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。このキーセットはＤＮＫ（Device Node Key）と呼ばれるが、その具体例については後に説明する。図１の最下段に示すＫ０００～Ｋ１１１１が各デバイスＤＶ０～ＤＶ１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）に続いて、最下段から２番目の節（ノード）に記載されたキー：Ｋ０～Ｋ

１１１をノードキーとする。なお文言上「ルートキー」も「ノードキー」に含むことがある。

【００３６】図１に示すツリー構成において、例えばデバイスＤＶ０は上記ＤＮＫとして、リーフキーＫ０００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ルートキーＫＲを所有する。例えばＤＮＫにおいてはノードキー：Ｋ０００、Ｋ００、Ｋ０、ルートキーＫＲをリーフキーＫ００００によって暗号化した状態で所有する。デバイスＤＶ５は同様の方式で、リーフキーＫ０１０１、ノードキーＫ０１０、Ｋ０１、Ｋ０、ルートキーＫＲを所有する。デバイスＤＶ１５も同様の方式で、リーフキーＫ１１１１、ノードキーＫ１１１、Ｋ１１、Ｋ１、ルートキーＫＲを所有する。なお、図１のツリーにはデバイスがＤＶ０～ＤＶ１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００３７】また、図１のツリー構造に含まれる各情報処理装置（デバイス）には、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプの情報処理装置が含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００３８】これらの様々な情報処理装置（デバイス）、アプリケーションが共存するシステムにおいて、例えば図１の点線で囲んだ部分、すなわちデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１の点線で囲んだ部分、すなわちデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【００３９】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【００４０】このツリー構造において、図１から明らかなように、１つのグループに含まれる３つのデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３はノードキー／ルートキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーＣＫをノードキーＫ００で暗号化した値Ｅ（Ｋ００，ＣＫ）を、ネットワークを介してあるいは記録媒体に格納してデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３に配布すれば、デバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅ（Ｋ００，ＣＫ）を解いてコンテンツキーＣＫを得ることが可能となる。

【００４１】また、ある時点ｔにおいて、デバイスＤＶ３の所有するキーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３のグループ）で送受信されるデータを守るために、デバイスＤＶ３をシステムから切り離す必要がある。そのためには、ノードキーＫ００１，Ｋ００，Ｋ０、ルートキーＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイスＤＶ０，ＤＶ１，ＤＶ２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Ｇｅｎｅｒａｔｉｏｎ）：ｔの更新キーであることを示す。もちろんコンテンツ配信に際して、他の事情、例えば著作権者側の要望やシステム配信上の都合などの各種事情に応じて、ノードキーやルートキーＫＲを更新する場合もある。これらのことから、正規のデバイスに対してキー更新を伝える必要がある。

【００４２】更新キーの配布処理について説明する。キーの更新は、例えば、図２（ａ）に示す有効化キーブロック（ＥＫＢ：Ｅｎａｂｌｉｎｇ Ｋｅｙ Ｂｌｏｃｋ）と呼ばれるブロックデータによって構成されるテーブルを、たとえばネットワーク、あるいは記録媒体に格納してデバイスに供給することによって実行される。例えば上記のようにデバイスＤＶ３を切り離す場合は、ＥＫＢをデバイスＤＶ０，ＤＶ１，ＤＶ２に供給する。なお、有効化キーブロック（ＥＫＢ）は、図１に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化

キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれることもある。

【００４３】図２（ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図２の例は、図１に示すツリー構造中のデバイスＤＶ０，ＤＶ１，ＤＶ２において、世代もの更新ノードキーを配布することを目的として形成されたブロックデータである。例えば上記のようにキーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが不正に露呈された場合を想定すると、デバイスＤＶ０，デバイスＤＶ１は、更新キーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要となり、デバイスＤＶ２は、更新キーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要となる。

【００４４】図２（ａ）のＥＫＢに示されるように、この場合ＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイスＤＶ２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイスＤＶ２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図２（ａ）の下から２段目の暗号化キーＥ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下、図２（ａ）の上から２段目の暗号化キーＥ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０を得、さらに上から１段目の暗号化キーＥ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号し更新ルートキーＫ（ｔ）Ｒを得る。

【００４５】一方、デバイスＤＶ０，ＤＶ１においてそれぞれリーフキーＫ０００，Ｋ０００１、及びノードキーＫ０００は更新する対象に含まれておらず、更新キーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。このためデバイスＤＶ０，ＤＶ１では、それぞれ図２（ａ）の上から３段目の暗号化キーＥ（Ｋ０００，Ｋ（ｔ）００）を復号して更新ノードキーＫ（ｔ）００を取得し、また暗号化キーＥ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号して更新ノードキーＫ（ｔ）０を取得し、さらに暗号化キーＥ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号して更新ルートキーＫ（ｔ）Ｒを得る。このようにして、デバイスＤＶ０，ＤＶ１，ＤＶ２は更新したルートキーＫ（ｔ）Ｒを得ることができる。なお、図２（ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００４６】また、図１に示すツリー構造の上位段のノードキーＫ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図２（ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイスＤＶ０，ＤＶ１，ＤＶ２に配布することができる。

【００４７】図２（ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３がある記録媒体を用いており、新たな共通のコンテンツキーＣＫ（ｔ）が必要であるとする。このとき、デバイスＤＶ０，ＤＶ１，ＤＶ２，ＤＶ３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキーＣＫ（ｔ）を暗号化したデータＥ（Ｋ（ｔ）００，ＣＫ（ｔ））を図２（ｂ）に示すＥＫＢとともに配布する。この配布により、デバイスＤＶ４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。すなわち、デバイスＤＶ０，ＤＶ１，ＤＶ２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキーＣＫ（ｔ）を得ることが可能になる。

【００４８】以上のようにキー構造がツリー構造とされるとともに、上記例のようなＥＫＢによって任意に各キーを更新することが可能となる。このキー構造を用いることで、各種事情に応じてルートキーＫＲやノードキーを更新することも容易に可能となり、正規な状態でのコンテンツ配信がフレキシブルに実行できる。

【００４９】図３に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。４バイトでノードキーの数が示される。４バイトでノードキーの深さが示される。これは有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。４バイトでＥＫＢのバージョンが示される。なおバージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。リザーブは予備領域である。

【００５０】オフセットアドレスとして１６バイトの位置から、１６×Ｍバイトの領域にＥＫＢの実内容となる暗号化されたノードキー（１又は複数）が示される。つまり図２（ａ）（ｂ）で説明したような暗号化キーである。さらに、暗号化ＥＫＢバージョンや、電子署名（Signature）が示される。電子署名は、有効化キーブロック（ＥＫＢ）を発行したＥＫＢ発行局、例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【００５１】２．システム構成

上記のキー構造を採用した本発明の実施の形態について、以下説明していく。図４にシステム構成例を示す。本発明のデータ転送装置に相当するのは一次記録媒体側機器１であり、本発明のデータ記録装置に相当するのは二次記録媒体側機器２０Ａである。そして一次記録媒体

側機器１と二次記録媒体側機器２０Ａによりデータ転送システムが構築される。

【００５２】一次記録媒体側機器１は、例えばパーソナルコンピュータにより形成される。以下、説明の便宜上、一次記録媒体側機器１をパーソナルコンピュータ１と表記する場合もある。ただし一次記録媒体側機器１は、必ずしもパーソナルコンピュータによって形成されるものではない。この一次記録媒体側機器１は、例えばパーソナルコンピュータ上で起動されるＳＤＭＩコンテンツデータの蓄積／転送等を実行するソフトウエアによって、本発明でいうデータ転送装置としての動作を実行する。そしてパーソナルコンピュータ１に内蔵（又は外付け）のＨＤＤ５が一次記録媒体（及び一次記録媒体ドライブ手段）とされる。なお実施の形態の説明ではＨＤＤ５を一次記録媒体とするが、もちろん一次記録媒体に相当する記録メディアはＨＤＤに限られず、例えば光ディスク、光磁気ディスク等のメディア、機器内蔵の半導体メモリ、可搬型の半導体メモリ（メモリカード等）など、各種のものが考えられる。

【００５３】一次記録媒体側機器１は、通信ネットワーク１１０を介してコンテンツサーバ９１と通信可能とされ、これによって音楽等のコンテンツデータのダウンロードが可能とされる。もちろんコンテンツサーバ９１は複数存在し、パーソナルコンピュータ１のユーザーは多様なデータダウンロードサービスを任意に利用できるものである。コンテンツサーバ９１からパーソナルコンピュータ１にダウンロードされるコンテンツデータとしては、ＳＤＭＩ準拠のコンテンツデータもあれば、ＳＤＭＩに準拠していないコンテンツデータもある。

【００５４】ネットワーク１１０を形成する伝送路は、有線又は無線の公衆回線網とされてもよいし、パーソナルコンピュータ１とコンテンツサーバ９１の専用回線としてもよい。具体的にはネットワーク１１０としては、例えばインターネット、衛星通信網、光ファイバー網、その他各種の通信回線が適用できる。

【００５５】また、パーソナルコンピュータ１のＨＤＤ５には、内蔵or外付けのディスクドライブ装置によりＣＤ－ＤＡやＤＶＤなどのパッケージメディア９０（以下、ディスク９０ともいう）から再生された音楽等のコンテンツデータを蓄積させることもできる。

【００５６】パーソナルコンピュータ１には、二次記録媒体側機器２０Ａ又は２０Ｂを接続し、この二次記録媒体側機器２０Ａ又は２０Ｂに対して、ＨＤＤ５に蓄積したコンテンツデータを転送可能とされる。二次記録媒体側機器２０Ａ又は２０Ｂは、二次記録媒体に対する記録装置（記録再生装置）とされる。そしてパーソナルコンピュータ１から転送されてきたコンテンツデータを二次記録媒体にコピー記録できるものとされる。

【００５７】二次記録媒体側機器２０Ａ、２０Ｂの具体例としては各種考えられるが、ここでいう二次記録媒体側機器２０Ｂは、ＳＤＭＩ対応の記録装置である。このＳＤＭＩ対応の記録再生装置２０Ｂでは、二次記録媒体として、例えばフラッシュメモリ等の半導体メモリを利用したＳＤＭＩ対応のメモリカードが想定される。従って二次記録媒体側機器２０Ｂとは、例えばＳＤＭＩ対応のメモリカードに対する記録再生装置となる。この場合、二次記録媒体にはＳＤＭＩコンテンツが暗号化された状態で記録されるものとなる。またＳＤＭＩ対応の二次記録媒体にはＳＤＭＩコンテンツの識別子となるコンテンツＩＤを格納する管理情報フォーマットが形成されている。パーソナルコンピュータ１ではＨＤＤ５にコンテンツデータを格納する際に、そのアプリケーションによってコンテンツＩＤが発生され、コンテンツデータと共にＨＤＤ５に格納される。またチェックアウト／チェックインの管理もコンテンツＩＤを用いて行われるが、ＳＤＭＩ対応の二次記録媒体では、コンテンツデータを記録する場合には当該コンテンツＩＤも記録できるものとされる。

【００５８】一方、二次記録媒体側機器２０Ａは、ＳＤＭＩ対応ではないデータ記録装置に相当し、詳しくは後述するが、著作権保護が要求されるＳＤＭＩコンテンツを、暗号化を解いた状態で二次記録媒体に記録するものである。ここでの二次記録媒体の例としては、ミニディスクを挙げる。従って二次記録媒体側機器２０Ａは、ミニディスク記録再生装置とされる。以下、二次記録媒体側機器２０Ａを、記録再生装置２０Ａと表記する場合もある。この場合、ＳＤＭＩコンテンツを非暗号化状態で記録することによっても著作権保護機能が損なわれないように、後述する認証等がコピーの条件とされる。またこの場合のミニディスク等の二次記録媒体（つまり従来より普及しているメディア）には、コンテンツＩＤを格納する領域が用意されていない。このため後述するが、コンテンツＩＤについては、特別な管理方式が採られる。

【００５９】なお、二次記録媒体側機器２０Ａが記録再生するメディアはミニディスク以外にも、例えばフラッシュメモリ等の半導体メモリを利用したメモリカードや、光磁気ディスクとしてのミニディスク、或いはＣＤ－Ｒ（CD Recordable）、ＣＤ－ＲＷ(CD Rewitable)、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷなどが考えられる。従って、二次記録媒体側機器２０Ａとしては、これらのメディアに対応する記録装置であればよい。

【００６０】パーソナルコンピュータ１と二次記録媒体側機器２０Ａ又は２０Ｂとは、例えばＵＳＢ（Universal Serial Bus）、ＩＥＥＥ１３９４などの伝送規格に基づく接続が行われる。もちろん他の伝送規格の有線伝送路、或いは無線伝送路によりコンテンツデータ等の転送が可能とされるものでもよい。

【００６１】３．ＳＤＭＩコンテンツのデータパス

例えば図４のようなシステムを想定した場合の、ＳＤＭ

Ｉで策定されたデータパスを図５に示す。なお、このデータパスは、例えば一次記録媒体としてのＨＤＤ５を備えたパーソナルコンピュータ１において、音楽コンテンツの蓄積及び外部機器（二次記録媒体側機器２０Ａ、２０Ｂ）への転送処理についてのデータパスであり、換言すればパーソナルコンピュータ１において音楽コンテンツの蓄積／転送処理を行うソフトウエアにより実現されるものである。図５のデータパス上の手順／処理はＤＰ１～ＤＰ９の符号を付しており、以下の説明では対応箇所をこの符号で示す。

【００６２】図４に示したネットワーク１１０を介して外部サーバ９１から配信されたコンテンツデータ（ネットワークコンテンツ）は、まずそれがＳＤＭＩに準拠した著作権保護されるコンテンツであるか否かが確認される（ＤＰ１）。配信されるネットワークコンテンツとしては、サーバ側がＳＤＭＩに準拠したコンテンツとして送信してくるもの（以下、ＳＤＭＩ準拠コンテンツ）と、ＳＤＭＩとは無関係なコンテンツ（以下、非ＳＤＭＩコンテンツ）がある。

【００６３】そしてＳＤＭＩ準拠コンテンツの場合は、そのデータは例えばＤＥＳ等の鍵暗号によって、コンテンツ鍵ＣＫで暗号化されている。コンテンツデータ自体は、元々はＡＴＲＡＣ３などの圧縮方式でエンコードされたデータ（Ａ３Ｄ）であるとすると、ＳＤＭＩ準拠コンテンツは、Ｅ（ＣＫ，Ａ３Ｄ）の状態で配信される。

【００６４】配信されたネットワークコンテンツがＳＤＭＩ準拠コンテンツであった場合は、一次記録媒体であるＨＤＤ５にＳＤＭＩコンテンツとして蓄積される（ＤＰ１→ＤＰ２）。この場合、コンテンツデータは配信されたＥ（ＣＫ，Ａ３Ｄ）の状態でＨＤＤ５に書き込まれる。或いは、暗号化が一旦復号された後、別の鍵ＣＫ’で暗号化が行われ、つまり鍵の掛け替えが行われて、Ｅ（ＣＫ’，Ａ３Ｄ）の状態でＨＤＤ５に書き込まれることもある。

【００６５】一方、ネットワークコンテンツが非ＳＤＭＩコンテンツであった場合は、ウォーターマークチェック、即ち電子透かしによるスクリーニング処理が行われる（ＤＰ１→ＤＰ３）。さらに、例えばパーソナルコンピュータ１に装備されているＣＤ－ＲＯＭドライブ等の内蔵ドライブ、或いはパーソナルコンピュータ１と接続されたディスクドライブ装置において再生されるＣＤ－ＤＡ、ＤＶＤ等のパッケージメディアから読み出されたコンテンツデータ（ディスクコンテンツ）については、直接ウォーターマークチェックが行われる（ＤＰ３）。つまりＳＤＭＩに準拠していないコンテンツデータについては、ウォーターマークチェックが行われることになる。

【００６６】もしウォーターマークチェックに合格しない場合は、そのコンテンツデータはＳＤＭＩデータパス上でコピー不可扱いとなる（ＤＰ３→ＤＰ５）。具体的な扱いはソフトウエア設計により多様に考えられるが、例えばＨＤＤ５には格納するが、他のメディアへのコピー／ムーブのための転送が不可能なコンテンツデータと扱われるようにしたり、或いはＳＤＭＩ準拠のコンテンツ処理上においてＨＤＤ５に格納されないものとすることが考えられる。

【００６７】ウォーターマークチェックに合格した場合、即ち電子透かしが存在し、かつコピーコントロールビットとしてコピー許可が確認された場合は、合法的にコピー可能なコンテンツデータと判断され、続いてその コンテンツデータをＳＤＭＩ扱いとするか否かが確認される（ＤＰ４）。このようなコンテンツデータをＳＤＭＩに準拠したものとして扱うか否かは、ソフトウエア設計やユーザー設定などに応じたものとすればよい。

【００６８】ＳＤＭＩ扱いとしない場合は、非ＳＤＭＩ扱いとして当該ＳＤＭＩに準拠したコンテンツデータパスからは除外される（ＤＰ６）。例えばＳＤＭＩに対応しない記録装置への転送等を可能としてもよい。一方、ＳＤＭＩ扱いとする場合は、そのコンテンツデータは暗号化され、ＳＤＭＩコンテンツとしてＨＤＤ５に蓄積される（ＤＰ４→ＤＰ２）。例えばＥ（ＣＫ，Ａ３Ｄ）の状態、又はＥ（ＣＫ’，Ａ３Ｄ）の状態でＨＤＤ５に蓄積される。

【００６９】以上のデータパスにより、一次記録媒体としてのＨＤＤ５には、ネットワーク１１０を介して得られたＳＤＭＩ扱いのコンテンツ（ＳＤＭＩネットワークコンテンツ）や、ＣＤ－ＤＡなどのディスク或いは他のメディアから取り出したＳＤＭＩ扱いのコンテンツ（ＳＤＭＩディスクコンテンツ）が蓄積されるものとなる。またＳＤＭＩコンテンツについては、コンテンツ毎の後述するUsage Ruleの管理などのために、コンテンツ毎にユニークなデータとなるコンテンツＩＤが生成され、ＨＤＤ５に記憶される。

【００７０】ＨＤＤ５に格納されたＳＤＭＩコンテンツ（ＳＤＭＩネットワークコンテンツ又はＳＤＭＩディスクコンテンツ）は、所定のルールのもとで、ＳＤＭＩ対応の記録再生装置２０Ｂに対して転送し、ＳＤＭＩ対応の二次記録媒体にコピー可能とされる。また本例の場合はＳＤＭＩ対応の記録再生装置２０Ｂ以外に、記録再生装置２０Ａにも、所定の条件の下で転送可能となる。

【００７１】まず、ＨＤＤ５を有するパーソナルコンピュータ１にＳＤＭＩ対応の記録再生装置２０Ｂが接続されている場合は、以下のようになる。ＳＤＭＩディスクコンテンツの場合は、ＳＤＭＩディスクコンテンツに対応する転送の扱いのルール（Usage Rule）が決められており、その扱いルールのもとで、ＳＤＭＩ対応の記録再生装置２０Ｂに対してコピーのための転送が認められる（ＤＰ８）。なおこのデータパスにおいて、一次記録媒体（ＨＤＤ５）からＳＤＭＩ対応記録再生装置２０Ｂ（又は２０Ａ）で記録再生される二次記録媒体（メモリ

カード等）に対してのコピー転送が「チェックアウト」であり、逆に二次記録媒体からの一次記録媒体へのムーブ転送が「チェックイン」である。なお二次記録媒体から一次記録媒体へのムーブの場合は、二次記録媒体上では当該コンテンツデータは消去された状態となる。

【００７２】ＳＤＭＩディスクコンテンツに対応する転送の扱いルールとしては、１つのコンテンツデータにつき例えば３回までのチェックアウトが許されるなど、所定のチェックアウト上限回数が定められている。従って、例えばＳＤＭＩ対応の３つの二次記録媒体まではコピー（チェックアウト）が許可される。またチェックインが行われた場合は、そのコンテンツデータについてのチェックアウト回数が減算されるものとなる。従って、例え３つのＳＤＭＩ対応二次記録媒体にコピーした後であっても、そのうちの１つの二次記録媒体からチェックインさせれば、そのコンテンツはさらにもう一度、ＳＤＭＩ対応二次記録媒体にコピー可能とされる。つまり、常に最大３つのＳＤＭＩ対応二次記録媒体にコンテンツデータが併存することが許されるものとなる。

【００７３】ＳＤＭＩネットワークコンテンツの場合も、ＳＤＭＩネットワークコンテンツに対応する転送の扱いのルール（Usage Rule）が決められており、その扱いルールのもとで、ＳＤＭＩ対応の記録再生装置２０Ｂに対してコピーのための転送が認められる（ＤＰ７）。この扱いルールとしては、上記同様にチェックアウト回数の上限等が決められるものであるが、その上限回数などは、ＳＤＭＩディスクコンテンツの場合の扱いルールと同様としてもよいし、異なる回数としてもよい。例えばチェックアウト上限を１回とすることが考えられる。その場合は、１つのコンテンツデータにつき、他の１つのＳＤＭＩ対応の二次記録媒体にしかコピーできないが、その二次記録媒体からチェックインすれば、再度コピー転送が可能となる。

【００７４】これらの扱いルールに従って、ＳＤＭＩ対応の二次記録媒体に対してコピーするためにＳＤＭＩコンテンツが転送される場合は、その伝送線路上では暗号化状態のままデータ伝送が行われる。つまり例えば上記のＥ（ＣＫ，Ａ３Ｄ）の状態ＲはＥ（ＣＫ'，Ａ３Ｄ）の状態で転送される。さらに、暗号化されて伝送されてきたＳＤＭＩコンテンツを受信したＳＤＭＩ対応記録再生装置２０Ｂでは、そのＳＤＭＩコンテンツを暗号化状態のままで二次記録媒体にコピー記録することになる。

【００７５】ＳＤＭＩ対応記録再生装置２０Ｂが、二次記録媒体にコピー記録されたＳＤＭＩコンテンツを再生する場合は、二次記録媒体から読み出したコンテンツデータの暗号化を復号して再生する。つまりＥ（ＣＫ，Ａ３Ｄ）の状態ＲはＥ（ＣＫ'，Ａ３Ｄ）の状態で二次記録媒体に記録されたコンテンツデータを、鍵ＣＫ、又は鍵ＣＫ'による復号処理を行う。即ちＤ｛ＣＫ，Ｅ（ＣＫ，Ａ３Ｄ）｝＝Ａ３Ｄ、又はＤ｛ＣＫ'，Ｅ（ＣＫ'，Ａ３Ｄ）｝＝Ａ３Ｄ、として暗号解読されたＡＴＲＡＣ３データ（Ａ３Ｄ）として元のコンテンツデータを得る。このコンテンツデータについてはＡＴＲＡＣ３圧縮に対する伸張処理等を行うことで、例えばオーディオデータとして復調し、音楽等の再生出力を行う。

【００７６】以上のように、ＳＤＭＩ準拠のコンテンツデータは、ＳＤＭＩ対応の記録再生装置２０Ｂにチェックアウトされるまでのデータパス、さらには二次記録媒体上に至るまで、暗号化が施されたデータとなっていることや、上記転送の扱いルールチェックによるコピー管理が行われることで、コンテンツデータについての適切な著作権保護が可能となる。

【００７７】一方、パーソナルコンピュータ１に、記録再生装置２０Ａが接続されている場合は、次のような処理が採られる。なお上記のように、記録再生装置２０Ａは、ＳＤＭＩ対応の記録再生装置２０Ｂとは異なって、二次記録媒体としての例えばミニディスクなどに、暗号化を解いた状態で記録するものである。暗号化を解いた状態で記録することにより、そのミニディスクにコピー記録されたコンテンツデータは、一般に普及している通常のミニディスク再生装置によっても再生可能となり、これによってユーザーの利便性を向上させることができる。但し、暗号化を解いた状態で記録することは、著作権保護の点で不都合が生じる。そこで、記録再生装置２０Ａにコンテンツデータを転送する場合には、所定の条件を満たすことが必要とされる。

【００７８】ＳＤＭＩネットワークコンテンツを記録再生装置２０Ａに転送して暗号化を解いた状態で二次記録媒体にコピー記録することを許可する条件としては、例えば、①記録再生装置２０Ａが認証ＯＫとなったこと、②転送しようとするコンテンツデータについてコピー記録を著作権者側が認めていること、③チェックアウト／チェックインとして転送の扱いのルール（Usage Rule）を満たすことの３つとされる。この①②③の転送条件が満たされていることでＳＤＭＩ対応記録再生装置２０Ｂ以外の機器に対しても、無制限なコピー転送はできず、著作権保護機能も確保される。また、転送を行う伝送路上では暗号化状態とされること（記録再生装置２０Ａ側で暗号解読を行う）でも著作権保護機能を与えることができる。

【００７９】ＳＤＭＩネットワークコンテンツを記録再生装置２０Ａに転送する場合には、上記①②③の転送条件がチェックされる（ＤＰ９）。即ち記録再生装置２０Ａについて所定の認証処理が行われる。また、コンテンツデータに含まれるフラグ情報などから、著作権者側のコピー許可の意志が確認される。さらにチェックイン／チェックアウトの扱いルールが課される。

【００８０】これらの条件に従って、ＳＤＭＩネットワークコンテンツを記録再生装置２０Ａに転送する場合は、その伝送線路上では暗号化状態のままデータ伝送が

行われる。つまり例えば上記のE（CK，A3D）の状態又はE（CK'，A3D）の状態で転送される。そしてこの暗号化されたSDMIネットワークコンテンツは、後述する図7の構成の記録再生装置20Aにおいて受信処理された後、復号処理部28で暗号化が復号され、例えば元のATRAC3圧縮データ（A3D）とされる。そしてその暗号化が解かれたコンテンツデータが、図7のエンコード／デコード部24によるエンコード処理を経て記録／再生部25に供給され、ミニディスク100にコピー記録されるものとなる。

【0081】従って記録再生装置20Aが、ミニディスク100にコピー記録したSDMIコンテンツを再生する場合は、ミニディスク100から読み出したデータについて通常のミニディスクシステムでのデコード処理、つまりEFM復調、ACIRCエラー訂正、ATRAC圧縮方式に対する伸張処理等を行えばよい。これは、当該コピー記録されたミニディスク100は、通常のミニディスク再生装置に装填した場合も、コンテンツデータが通常に再生できるものとなっていることを意味する。つまりユーザーは、上述したように、ミニディスク100にコピー記録したSDMIネットワークコンテンツを、SDMI非対応の通常のミニディスク再生装置で再生させ、音楽等を楽しむことができる。

【0082】なお、図5のデータパスにおいて、DP7，DP8，DP9の扱いルールチェック等によって転送許可がされない場合は、記録再生装置20A、20Bに対する転送が行われないことはいうまでもない。

【0083】4．データ転送装置の構成例（一次記録媒体側機器／PC）

図6に、データ転送装置となる一次記録媒体側機器1の構成を示す。なお、ここで説明する例は、パーソナルコンピュータにより一次記録媒体側機器1を形成する場合であるが、同様の機能を持つ構成が専用のハードウエアにより構築されるなどにより、データ転送専用の機器として形成されてもよい。

【0084】本例の場合は、パーソナルコンピュータ1にデータ転送装置としての機能を実行させるソフトウエアプログラムがインストールされることでデータ転送装置となる一次記録媒体側機器が実現される。なお、本明細書で「パーソナルコンピュータ」又は「コンピュータ」といっているのは、いわゆる汎用コンピュータとしての広義の意味である。当該プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク（HDD）5やROM3に予め記録しておくことができる。あるいはまた、プログラムは、フロッピー（登録商標）ディスク、CD－ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体90に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体90は、いわゆるパッケージソフトウェアとして提供することができる。

【0085】なお、プログラムは、上述したようなリムーバブル記録媒体90からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部8で受信し、内蔵するHDD5にインストールすることができる。

【0086】図6のコンピュータ1は、CPU(Central Processing Unit)2を内蔵している。CPU2には、バス12を介して、入出力インタフェース10が接続されている。CPU2は、入出力インタフェース10を介して、ユーザによって、キーボードや、マウス、マイク等で構成される入力部7が操作等されることにより指令が入力されると、それに従って、ROM(Read Only Memory)3に格納されているプログラムを実行する。あるいはまた、CPU2は、HDD5に格納されているプログラム、衛星着しくはネットワークから転送され、通信部8で受信されてHDD5にインストールされたプログラム、またはドライブ9に装着された光ディスク等のリムーバブル記録媒体90から読み出されてHDD5にインストールされたプログラムを、RAM(Random Access Memory)4にロードして実行する。これにより、CPU2は、後述するSDMIコンテンツに対してのデータ転送装置としての処理を実行する。そしてCPU2は、その処理結果を、必要に応じて、例えば入出力インタフェース10を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部6から出力、あるいは通信部8から送信、さらにはHDD5に記録等させる。

【0087】本例の場合、通信部8は、図4のネットワーク110を介した各種サーバとの通信が可能とされる。即ちコンピュータ1は、外部のコンテンツサーバ91から音楽コンテンツ等のネットワークコンテンツのダウンロードが可能とされる。ダウンロードされるネットワークコンテンツは、上述したデータパスに則って、SDMI対応のコンテンツとしての処理、もしくはSDMI非対応のコンテンツとしての処理が行われ、例えば少なくともSDMI対応の処理としてはSDMIコンテンツとしてHDD5に蓄積される。HDD5に蓄積されたSDMIコンテンツは、SDMI対応の二次記録媒体側機器20B、又は認証された二次記録媒体側機器（記録再生装置）20Aに対する転送対象のコンテンツとなる。

【0088】接続部11は、二次記録媒体側機器20A、20Bとの間でデータ通信可能に接続される部位である。例えばUSBインターフェース、IEEE1394インターフェースなどの例が考えられる。もちろん他

の規格の有線インターフェースや、赤外線や電波を用いた無線インターフェースであってもよい。

【0089】なお、図5で説明したデータパスを実現するための各種処理は、それぞれ時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。また、プログラムは、1つのコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0090】5．データ記録装置の構成例（二次記録媒体側機器／記録再生装置）

二次記録媒体側機器（記録再生装置）20Aの構成例を図7に示す。この例は、記録再生装置20Aを例えばミニディスクレコーダとして構成したものである。従って二次記録媒体100は、ミニディスク（光磁気ディスク）の例となる。以下「ミニディスク100」とも表記する。なお、図7においては、二次記録媒体100としてのミニディスクに対する記録再生データの処理系、及び上記一次記録媒体側機器1からのデータ転送に対する処理系のみを示し、ミニディスク100に対する駆動系、サーボ系、再生出力系等は通常のミニディスク記録再生装置と同様であるため詳しい図示を省略している。

【0091】MD制御部（CPU）21は記録再生装置20Aにおいてミニディスク100に対しての記録再生動作の制御を行うコントローラとなる。具体的には、ミニディスク100に対する記録再生のために、回転駆動、スピンドルサーボ、フォーカスサーボ、トラッキングサーボ、スレッドサーボなどの制御、光学ヘッド／磁気ヘッドのレーザ光や磁界印加動作の制御、記録再生データのエンコード／デコード処理の制御などを行う。

【0092】記録／再生部25は、光学ヘッド、磁気ヘッド、ディスク回転駆動系、サーボ系等が備えられ、実際にミニディスク100に対してデータの記録／再生を行う部位である。

【0093】エンコード／デコード部24は、ミニディスク100に対する記録データのエンコード、及びミニディスク100から再生された再生データのデコードを行う。公知のようにミニディスクシステムの場合は、記録データはACIRCエラー訂正符号のエンコード処理やEFM変調処理が施される。エンコード／デコード部24は、記録データに対してACIRCエンコード及びEFMエンコードを行って記録／再生部25に供給することになる。また再生時には、記録／再生部25から読み出されて供給されてきたデータ（RF信号）に対して二値化処理、EFM復調、ACIRC方式のエラー訂正処理などのデコード処理を行うことになる。

【0094】バッファメモリ30は、ミニディスク100に対する記録データ、再生データのバッファリングを行う。特にショックプルーフ機能として知られているバッファリング機能も行う。データ記録時には、バッファメモリ30にはATRAC／ATRAC3方式の圧縮符号化された記録データが一旦蓄積される。そして所定データ量毎に間欠的に読み出されてエンコード／デコード部24に供給され、記録処理に供される。またデータ再生時には、ミニディスク100から読み出され、エンコード／デコード部24でデコードされたデータが一旦蓄積される。そして、蓄積されたデータは連続的に読み出されてコーデック23での圧縮デコード処理に供される。

【0095】コーデック23は、ATRAC／ATRAC3方式の圧縮符号化による圧縮処理、及び伸張処理を行う部位である。ミニディスク100に記録されるデータは、ATRAC／ATRAC3方式の圧縮符号化が行われた後、上記エンコード処理が施されたものである。従って当該記録再生装置20Aに、圧縮符号化がされていないデータ、例えばPCMオーディオデータ等が記録データとして入力された場合は、コーデック23でATRAC方式又はATRAC3方式の圧縮符号化が行われ、その圧縮データがエンコード／デコード部24に供給されることになる。また再生時には、記録／再生部25で読み出され、エンコード／デコード部24でデコードされたデータは、ATRAC／ATRAC3方式の圧縮符号化状態のデータである。このデータがバッファメモリ30を介してコーデック23に供給され、コーデック23でATRAC／ATRAC3方式の圧縮に対する伸張処理が行われることで、例えば44．1KHz、16ビット量子化のデジタルオーディオデータが復調される。このデジタルオーディオデータは、図示しない出力系の回路において、例えばD／A変換、アナログ信号処理、増幅処理等が行われて、スピーカ出力信号とされ、音楽等として再生される。或いは、デジタルオーディオデータの状態で他の機器に対して出力可能とすることもできる。

【0096】以上の構成は、通常のミニディスクシステムの記録再生装置にも備えられる構成要素であるが、本例の記録再生装置20Aでは、一次記録媒体側機器1としてのパーソナルコンピュータに対応する部位がさらに設けられる。すなわち転送されてくるコンテンツデータについての受信・復号等の処理を行う部位として、通信部26、DMA27、復号処理部28、キャッシュメモリ29、フロー制御部31、システム制御部32が設けられる。

【0097】システム制御部32（CPU）は、当該記録再生装置20Aの全体の制御を行う部位である。例えば、パーソナルコンピュータ1との間の認証のための通信やデータ生成の指示や、パーソナルコンピュータ1からの各種コマンドのやりとり、転送されてくるコンテンツデータに対する処理などの制御を行う。またそれらの

制御に応じてMD制御部21に指示を出し、ミニディスク100に対するコンテンツデータの記録／再生、管理情報の読出や更新などの制御も行う。また図示していないが、ユーザーインターフェースとして操作部や表示部が設けられるが、操作部からのユーザー操作の監視及び操作に応じた処理や、表示部の表示制御なども行う。

【0098】通信部26は、図6のパーソナルコンピュータ1の接続部11との間で接続され、パーソナルコンピュータ1との間でデータ通信を行う部位である。例えばUSB又はIEEE1394などの通信方式に対応する信号処理を行う。通信部26によって受信されるパーソナルコンピュータ1からの通信としては、各種コマンド及びSDMIコンテンツなどがある。

【0099】通信部26で受信されたSDMIコンテンツとしてのデータは、DMA（Direct Memory Access）27の制御により、キャッシュメモリ29に格納されていく。なおもちろん、DMA27ではなくCPU制御によって、キャッシュメモリ29へのデータ移動を行うようにしてもよい。

【0100】復号処理部28は、SDMIコンテンツの暗号化処理に対応するための部位である。即ちキャッシュメモリ29に記憶されたコンテンツデータについての暗号解読処理を行う。そして非暗号化状態に解読したコンテンツデータは、キャッシュメモリ29の別の領域に記憶していく。

【0101】SDMIコンテンツはコンテンツキーCK又はCK'で暗号化されているため、少なくともコンテンツキーCK、CK'を認識できる情報が記憶される。具体的には後述するが、上記図1の説明で言及したDNK（Device Node Key）が記憶されることになる。この記録再生装置20Bは、図1における1つのデバイス（DVx）に相当するものとなるが、そのため、DNKにおいてリーフキーや、リーフキーによって暗号化されたノードキー、ルートキーが記憶されるものとなる。そしてそのようなDNKを用いて、また場合によっては送信されてくる上述したEKBを用いて、コンテンツキーCKを認識できる。

【0102】SDMIコンテンツに対するコンテンツキーCKを認識可能な情報であるDNKが記憶されていることで、復号処理部28は、コンテンツキーCKで暗号化された状態で送信されてきたてSDMIコンテンツ、即ち例えばE（CK、A3D）の状態のコンテンツを、復号することができる。つまりD｛CK，E（CK、A3D）｝＝A3Dとして、復号されたATRAC3圧縮状態のデータを得ることができる。このようにして復号されたATRAC3圧縮データは、エンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録できる。

【0103】なお、SDMIコンテンツは、必ずしもATRAC3圧縮データが暗号化されたものではない。例えばリニアPCMデータが鍵CKで暗号化されたものなども考えられる。つまり例えばE（CK、PCM）の状態のコンテンツが転送入力去る場合もある。その場合は、当然ながら復号処理部でD｛CK，E（CK、PCM）｝＝PCMとして、復号されたリニアPCMデータが得られる。その場合は、当該PCMデータは、コーデック23でATRAC3圧縮処理が行われた後、エンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録できる。

【0104】復号処理部28は、さらに認証処理のための鍵を記憶する場合もある。後述する認証処理例では記録再生装置20Aが記憶している公開鍵P、秘密鍵Sを使用する。その場合は公開鍵P、秘密鍵Sも、復号処理部28に記憶されることになる。また秘密鍵Sを用いた暗号化処理も行う。

【0105】また復号処理部28は、ハッシュエンジンも搭載しており、いわゆるハッシュ（HASH）関数演算により、コンテンツIDを生成する処理も行う。なお、このコンテンツIDの生成については後に詳述する。

【0106】暗号化が解除されたSDMIコンテンツデータ、例えばATRAC3方式の圧縮データや、PCMデータの状態のコンテンツデータは、キャッシュメモリ29からフロー制御部31に転送されることになる。フロー制御部31は、暗号化解除されたSDMIコンテンツデータを、ミニディスク100に対して記録するために、記録処理系であるMD制御部21側（コーデック23、エンコード／デコード部24、記録／再生部25、バッファメモリ30側）に転送する部位である。そして、MD制御部21からのリクエスト（XARQ）に応じてデータを転送していく。このフロー制御部31によって、コンテンツデータの受信、暗号解読処理、及びミニディスク100に対する記録処理の間のタイミング的な調整がはかられる。

【0107】以上の構成により、パーソナルコンピュータ1から送信されたSDMIコンテンツデータとしてE（CK、A3D）の状態のデータ、又はE（CK、PCM）の状態のデータは、非暗号化状態とされ、ATRAC3圧縮データの状態でエンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録されるものとなる。

【0108】ところで、パーソナルコンピュータ1から記録再生装置20Aに対しては、コンテンツデータのチェックアウト／チェックイン、その他の通信セッションの際には、各種コマンドも送信してくる。これらのコマンドはレシーバ26によって受信されるとシステム制御部32に伝えられ、システム制御部32は、これらのコマンドに応じて各種処理を行うと共に、コマンドに対するレスポンスを通信部26からパーソナルコンピュータ1に対して送信する。

【0109】6．ミニディスクの管理方式

ここで、ミニディスク１００に記録されるデータ及び管理情報について説明しておく。ミニディスクシステムのようなデジタル記録／再生システムでは、記録媒体にデータの記録動作や再生動作を制御するための管理情報としてＴＯＣ（Table ofContents）が記録されており、記録再生装置側では予めディスク等の記録媒体からこのＴＯＣ情報を読み出してメモリに保持しておき、記録再生動作の際に、このＴＯＣ情報を参照して記録位置や読出位置を把握して記録再生のためのアクセス動作を実行できるようにしている。

【０１１０】ミニディスクの場合、ＴＯＣ情報としては書き換え不能な情報としてピットにより記録されるＰ－ＴＯＣ（プリマスタードＴＯＣ）と、楽曲等の記録、消去などに応じて書き換えられるように光磁気記録されているＵ－ＴＯＣ（ユーザーＴＯＣ）が存在し、Ｕ－ＴＯＣについては、記録／消去に応じてまずメモリ内でデータを更新し、この更新データで所定タイミングでディスク上のＵ－ＴＯＣ領域を書き換えていくことになる。なおＵ－ＴＯＣには、ディスク上に記録されるオーディオデータ等のコンテンツデータがトラックと呼ばれる単位で管理される。つまり１つのトラックは、例えば１つの楽曲に相当するものとなる。

【０１１１】まず、ミニディスク１００に記録されるデータとして、クラスタというデータ単位について説明する。ミニディスクシステムでは記録データとして１クラスタという単位毎のデータストリームが形成されるが、この記録動作の単位となるクラスタのフォーマットは図８に示される。ミニディスクシステムでの記録トラックとしては図８のようにクラスタＣＬが連続して形成されており、１クラスタが記録時の最小単位とされる。

【０１１２】そして１クラスタＣＬは、セクターＳＣＦＣ～ＳＣＦＥとして示す３セクターのリンキングセクターと、セクターＳＣＦＦとして示す１セクターのサブデータセクターと、セクターＳＣ００～ＳＣ１Ｆとして示す３２セクターのメインセクターから形成されている。即ち１クラスタは３６セクターで構成される。１セクタは２３５２バイトで形成されるデータ単位である。

【０１１３】リンキングセクターＳＣＦＣ～ＳＣＦＥは、記録動作の切れ目としての緩衝領域や各種動作調整その他に用いられ、またサブデータセクターＳＣＦＦは、サブデータとして設定された情報の記録に用いることができる。そして、ＴＯＣデータ、オーディオデータ等の記録は３２セクターのメインセクターＳＣ００～ＳＣ１Ｆに行なわれる。

【０１１４】また、セクターはさらにサウンドグループという単位に細分化され、２セクターが１１サウンドグループに分けられている。つまり図示するように、セクターＳＣ００などの偶数セクターと、セクターＳＣ０１などの奇数セクターの連続する２つのセクターに、サウンドグループＳＧ００～ＳＧ０Ａが含まれる状態となっている。１つのサウンドグループは４２４バイトで形成されており、11.61msec の時間に相当する音声データ量となる。１つのサウンドグループＳＧ内にはデータがＬチャンネルとＲチャンネルに分けられて記録される。例えばサウンドグループＳＧ００はＬチャンネルデータＬ０とＲチャンネルデータＲ０で構成され、またサウンドグループＳＧ０１はＬチャンネルデータＬ１とＲチャンネルデータＲ１で構成される。なお、Ｌチャンネル又はＲチャンネルのデータ領域となる２１２バイトをサウンドフレームとよんでいる。

【０１１５】図９はミニディスク１００のエリア構造を示している。図９（ａ）はディスク最内周側から最外周側までのエリアを示しており、光磁気ディスクとしてのミニディスク１００は、最内周側はエンボスピットにより再生専用のデータが形成されるピット領域とされており、ここにＰ－ＴＯＣが記録されている。ピット領域より外周は光磁気領域とされ、記録トラックの案内溝としてのグループが形成された記録再生可能領域となっている。この光磁気領域の最内周側のクラスタ０～クラスタ４９までの区間が管理エリアとされ、実際の楽曲等がそれぞれ１つのトラックとして記録されるのは、クラスタ５０～クラスタ２２５１までのプログラムエリアとなる。プログラムエリアより外周はリードアウトエリアとされている。

【０１１６】管理エリア内を詳しく示したものが図９（ｂ）である。図９（ｂ）は横方向にセクター、縦方向にクラスタを示している。管理エリアにおいてクラスタ０，１はピット領域との緩衝エリアとされている。クラスタ２はパワーキャリブレーションエリアＰＣＡとされ、レーザー光の出力パワー調整等のために用いられる。クラスタ３，４，５はＵ－ＴＯＣが記録される。Ｕ－ＴＯＣの内容について詳しくは後述するが、１つのクラスタ内の３２個の各メインセクター（ＳＣ００～ＳＣ１Ｆ）においてデータフォーマットが規定され、それぞれ所定の管理情報が記録される。即ちプログラムエリアに記録されている各トラックのアドレス、フリーエリアのアドレス等が記録され、また各トラックに付随するトラックネーム、記録日時などの情報が記録できるようにＵ－ＴＯＣセクターが規定されている。このようなＵ－ＴＯＣデータとなるセクターを有するクラスタが、クラスタ３，４，５に３回繰り返し記録される。クラスタ４７，４８，４９は、プログラムエリアとの緩衝エリアとされる。なお斜線部ＰＤは、後述するプリペイド情報の記録領域として設定することができる。

【０１１７】クラスタ５０（＝１６進表記で３２ｈ）以降のプログラムエリアには、１つのクラスタ内の３２個の各メインセクター（ＳＣ００～ＳＣ１Ｆ）において、楽曲等の音声データがＡＴＲＡＣと呼ばれる圧縮形式で記録される。記録される各トラック（コンテンツデータ）や記録可能な領域は、Ｕ－ＴＯＣによって管理される。な

お、プログラム領域における各クラスタにおいて、セクターSCFFは、前述したようにサブデータとしての情報の記録に用いることができる。

【0118】図10によりU-TOCセクターについて説明する。なおP-TOCは図9で説明したようにディスク90の最内周側のピットエリアに形成されるもので、読出専用の情報である。そして、P-TOCによってディスクの記録可能エリア（レコーダブルユーザーエリア）や、リードアウトエリア、U-TOCエリアなどの位置の管理等が行なわれる。なお、全てのデータがピット形態で記録されている再生専用の光ディスクでは、P-TOCによってROM化されて記録されている楽曲の管理も行なうことができるようにされ、U-TOCは形成されない。P-TOCについては詳細な説明を省略する。

【0119】図10はU-TOCセクター0のフォーマットを示すものである。U-TOCセクターとしてはセクター0～セクター32まで設けることができる。即ち上記した1クラスタ内のメインセクターSC00～SC1Fに相当して記録されるセクターとなる。その中で、セクター1，セクター4は文字情報、セクター2は録音日時を記録するエリアとされている。これらセクター1、セクター2、セクター4については説明を省略する。

【0120】U-TOCセクター0は、記録された楽曲等のコンテンツデータ（トラック）や新たにコンテンツデータが録音可能なフリーエリアについての管理情報が記録されているデータ領域とされる。例えばミニディスク100に或る楽曲の録音を行なおうとする際には、MD制御部21は、U-TOCセクター0からディスク上のフリーエリアを探し出し、ここにデータを記録していくことになる。また、再生時には再生すべき楽曲が記録されているエリアをU-TOCセクター0から判別し、そのエリアにアクセスして再生動作を行なう。

【0121】図10のU-TOCセクター0のデータ領域（4バイト×588 の2352バイト）は、先頭位置にオール0又はオール1の1バイトデータが並んで形成される同期パターンが記録される。続いてクラスタアドレス(Cluster H) (Cluster L) 及びセクターアドレス(Sector)となるアドレスが3バイトにわたって記録され、さらにモード情報(MODE)が1バイト付加され、以上でヘッダとされる。ここでの3バイトのアドレスは、そのセクター自体のアドレスである。なお、同期パターンやアドレスが記録されるヘッダ部分については、このU-TOCセクター0に限らず、P-TOCセクター、プログラムエリアでのセクターでも同様であり、セクター単位にそのセクター自体のアドレス及び同期パターンが記録されている。

【0122】続いて所定バイト位置に、メーカーコード、モデルコード、最初のトラックのトラックナンバ(First TNO)、最後のトラックのトラックナンバ(Last TNO)、セクター使用状況(Used sectors)、ディスクシリアルナンバ、ディスクID等のデータが記録される。

【0123】さらに、ユーザーが録音を行なって記録されているトラック（楽曲等）の領域やフリーエリア等を後述するテーブル部に対応させることによって識別するため、ポインタ部として各種のポインタ(P-DFA, P-EMPTY , P-FRA , P-TN01～P-TN0255) が記録される領域が用意されている。

【0124】そしてポインタ(P-DFA～P-TN0255) に対応させることになるテーブル部として(01h) ～(FFh) までの255個のパーツテーブルが設けられ、それぞれのパーツテーブルには、或るパーツについて起点となるスタートアドレス、終端となるエンドアドレス、そのパーツのモード情報（トラックモード）が記録されている。さらに各パーツテーブルで示されるパーツが他のパーツへ続いて連結される場合があるため、その連結されるパーツのスタートアドレス及びエンドアドレスが記録されているパーツテーブルを示すリンク情報が記録できるようにされている。なおパーツとは1つのトラック内で時間的に連続したデータが物理的に連続して記録されているトラック部分のことをいう。そしてスタートアドレス、エンドアドレスとして示されるアドレスは、1つの楽曲（トラック）を構成する1又は複数の各パーツを示すアドレスとなる。これらのアドレスは短縮形で記録され、クラスタ、セクター、サウンドグループを指定する。

【0125】この種の記録再生装置では、1つの楽曲（トラック）のデータを物理的に不連続に、即ち複数のパーツにわたって記録されていてもパーツ間でアクセスしながら再生していくことにより再生動作に支障はないため、ユーザーが録音する楽曲等については、録音可能エリアの効率使用等の目的から、複数パーツにわけて記録する場合もある。

【0126】そのため、リンク情報が設けられ、例えば各パーツテーブルに与えられたナンバ(01h) ～(FFh) によって、連結すべきパーツテーブルを指定することによってパーツテーブルが連結できるようになされている。つまりU-TOCセクター0におけるテーブル部においては、1つのパーツテーブルは1つのパーツを表現しており、例えば3つのパーツが連結されて構成される楽曲についてはリンク情報によって連結される3つのパーツテーブルによって、そのパーツ位置の管理が行われる。なお、実際にはリンク情報は所定の演算処理によりU-TOCセクター0内のバイトポジションとされる数値で示される。即ち、304＋(リンク情報)×8（バイト目）としてパーツテーブルを指定する。

【0127】U-TOCセクター0のテーブル部における(01h) ～(FFh) までの各パーツテーブルは、ポインタ部におけるポインタ(P-DFA, P-EMPTY , P-FRA , P-TN01～P-TN0255) によって、以下のようにそのパーツの内容が示される。

【０１２８】ポインタP-DFAは光磁気ディスク９０上の欠陥領域について示しており、傷などによる欠陥領域となるトラック部分（＝パーツ）が示された１つのパーツテーブル又は複数のパーツテーブル内の先頭のパーツテーブルを指定している。つまり、欠陥パーツが存在する場合はポインタP-DFAにおいて(01h)～(FFh)のいづれかが記録されており、それに相当するパーツテーブルには、欠陥パーツがスタート及びエンドアドレスによって示されている。また、他にも欠陥パーツが存在する場合は、そのパーツテーブルにおけるリンク情報として他のパーツテーブルが指定され、そのパーツテーブルにも欠陥パーツが示されている。そして、さらに他の欠陥パーツがない場合はリンク情報は例えば『００ｈ』とされ、以降リンクなしとされる。

【０１２９】ポインタP-EMPTYはテーブル部における１又は複数の未使用のパーツテーブルの先頭のパーツテーブルを示すものであり、未使用のパーツテーブルが存在する場合は、ポインタP-EMPTYとして、(01h)～(FFh)のうちのいづれかが記録される。未使用のパーツテーブルが複数存在する場合は、ポインタP-EMPTYによって指定されたパーツテーブルからリンク情報によって順次パーツテーブルが指定されていき、全ての未使用のパーツテーブルがテーブル部上で連結される。

【０１３０】ポインタP-FRAは光磁気ディスク９０上のデータの書込可能なフリーエリア（消去領域を含む）について示しており、フリーエリアとなるトラック部分（＝パーツ）が示された１又は複数のパーツテーブル内の先頭のパーツテーブルを指定している。つまり、フリーエリアが存在する場合はポインタP-FRAにおいて(01h)～(FFh)のいづれかが記録されており、それに相当するパーツテーブルには、フリーエリアであるパーツがスタート及びエンドアドレスによって示されている。また、このようなパーツが複数個有り、つまりパーツテーブルが複数個有る場合はリンク情報により、リンク情報が『００ｈ』となるパーツテーブルまで順次指定されている。

【０１３１】図１１にパーツテーブルにより、フリーエリアとなるパーツの管理状態を模式的に示す。これはパーツ(03h)(18h)(1Fh)(2Bh)(E3h)がフリーエリアとされている時に、この状態がポインタP-FRAに引き続きパーツテーブル(03h)(18h)(1Fh)(2Bh)(E3h)のリンクによって表現されている状態を示している。なお上記した欠陥領域や未使用パーツテーブルの管理形態もこれと同様となる。

【０１３２】ポインタP-TNO1～P-TNO255は、ディスク９０にユーザーが記録を行なった楽曲などのトラックについて示しており、例えばポインタP-TNO1では第１トラックのデータが記録された１又は複数のパーツのうちの時間的に先頭となるパーツが示されたパーツテーブルを指定している。例えば第１トラックとされた楽曲がディスク上でトラックが分断されずに、つまり１つのパーツで記録されている場合は、その第１トラックの記録領域はポインタP-TNO1で示されるパーツテーブルにおけるスタート及びエンドアドレスとして記録されている。

【０１３３】また、例えば第２トラックとされた楽曲がディスク上で複数のパーツに離散的に記録されている場合は、その第２トラックの記録位置を示すため各パーツが時間的な順序に従って指定される。つまり、ポインタP-TNO2に指定されたパーツテーブルから、さらにリンク情報によって他のパーツテーブルが順次時間的な順序に従って指定されて、リンク情報が『００ｈ』となるパーツテーブルまで連結される（上記、図１１と同様の形態）。このように例えば２曲目を構成するデータが記録された全パーツが順次指定されて記録されていることにより、このＵ－ＴＯＣセクター０のデータを用いて、２曲目の再生時や、その２曲目の領域への上書き記録を行なう際に、記録再生ヘッドをアクセスさせ離散的なパーツから連続的な音楽情報を取り出したり、記録エリアを効率使用した記録が可能になる。

【０１３４】ところで、各パーツテーブルには１バイトのトラックモードが記録されるが、これはトラックの属性情報となる。１バイトを構成する８ビットを、ｄ１（ＭＳＢ）～ｄ８（ＬＳＢ）とすると、このトラックモードは次のように定義されている。

ｄ１・・・０：ライトプロテクテッド（上書消去、編集禁止）
１：ライトパーミッテッド
ｄ２・・・０：著作権有り、１：著作権無し
ｄ３・・・０：オリジナル、１：第１世代以上
ｄ４・・・０：オーディオデータ、１：未定義
ｄ５，ｄ６・・・０１：ノーマルオーディオ、その他：未定義
ｄ７・・・０：モノラル、１：ステレオ
ｄ８・・・０：エンファシスオフ、１：エンファシスオン

【０１３５】以上のように、書換可能な光磁気ディスク９０については、ディスク上のエリア管理はＰ－ＴＯＣによってなされ、またレコーダブルユーザーエリアにおいて記録された楽曲やフリーエリア等はＵ－ＴＯＣにより行なわれる。また、このようなＵ－ＴＯＣ構造により、ミニディスク１００に記録されたトラックについては、トラックの分割、複数トラックの１トラックへの連結、消去などの編集が、Ｕ－ＴＯＣを書き換えるのみで可能であることが理解される。

【０１３６】記録再生装置２０ＡにおいてＭＤ制御部２１は、記録／再生部２５にミニディスク１００が装填された際には、まずこのＴＯＣ情報を読み出すことにより、読み出したＵ－ＴＯＣ情報をバッファメモリ３０の特定のエリアに記憶させる。そして以後そのミニディスク１００に対する記録／再生／編集動作の際に参照でき

るようにしている。なお、コンテンツデータ（トラック）の記録や、記録されているトラックの編集などが行われる場合、U−TOCセクターの更新処理は、一旦バッファメモリ30に記憶されたU−TOCデータに対して行われる。そして所定時点でバッファメモリ30に記憶されている（更新された）TOC情報がミニディスク100に書き込まれることで、ディスク上でのU−TOC更新が行われる。

【0137】7．認証処理

SDMIデータパスの説明において言及したように、ミニディスク100に対して暗号化を解いた状態でコンテンツデータを記録する記録再生装置20Aについては、その転送／記録（チェックアウト）の条件の一つとして、パーソナルコンピュータ1からの認証がOKとならなければならない。認証とは、非暗号化状態でのコンテンツデータの記録動作が許可された機器として正当なものであるかを確認する処理となる。

【0138】この認証処理は、パーソナルコンピュータ1の接続部11に、SDMI対応記録再生装置20B以外の記録再生装置が接続された場合に行われる。なお、SDMI対応記録再生装置20Bが接続された場合は、その機器が本例でいうSDMI対応の記録再生装置20Bであることを確認する処理が行われる。即ち接続機器が、SDMI対応の記録再生装置20Bと確認されなかった場合に、以下説明する認証処理が行われ、記録再生装置20Aであるか否かが確認されるものとなる。

【0139】本例での認証処理は、非対称暗号（公開鍵暗号）を用いた認証方式を実行するものとしている。非対称暗号では、暗号化の鍵と復号化の鍵が異なる。いま、暗号前のデータをDb、暗号鍵をKe、復号鍵をKdとすると、暗号化データCは、C＝E（Ke，Db）で暗号化が行われ、またD（Kd，C）＝Dbでデータ Dbが復号される。ここで暗号鍵Ke、復号鍵Kdは鍵のペアと呼ばれ、一方は公開鍵として公開し、他方は秘密鍵として所定部位に保持されるものである。以下説明する認証処理では、鍵のペアKe、Kdのうちで公開鍵をP、秘密鍵をSとして表して説明する。上述したようにこの場合、記録再生装置20Aは、復号処理部28（又はシステム制御部32）に暗号鍵Ke、復号鍵Kdとなる、公開鍵P、秘密鍵Sを記憶していることになる。

【0140】認証処理に際しては、例えば一次記録媒体側機器（パーソナルコンピュータ）1のCPU2が、二次記録媒体側機器（記録再生装置）20Aのシステム制御部32に対して認証要求のコマンドを送信した後、CPU2（一次記録媒体側機器（パーソナルコンピュータ）1）と、システム制御部32（二次記録媒体側機器（記録再生装置）20A）の間で図12のような処理が行われることになる。

【0141】認証処理が開始されると、まず二次記録媒体側機器20Aのシステム制御部32は、処理S1として、復号処理部28に記憶している公開鍵Pをインターフェース部26から一次記録媒体側機器1に送信させる。なお、公開鍵Pは一次記録媒体側機器1側も知っている鍵である。従って、公開鍵Pについて両者が一致した認識が得られる場合は、当該処理S1は必ずしも実行されなくてもよい。一次記録媒体側機器1のCPU2は、公開鍵Pを受信したら、続いて処理S2として、乱数rを発生させる。そして処理S3として、二次記録媒体側機器20Aに乱数rを送信する。次に二次記録媒体側機器20Aのシステム制御部32は、処理S4として受信された乱数rを、復号処理部28に記憶された秘密鍵Sを用いて暗号化する。そして処理S5として、暗号化データE（S，r）を一次記録媒体側機器1に送信する。

【0142】一次記録媒体側機器1のCPU2は、暗号化データE（S，r）を受信したら、処理S6として、暗号化データE（S，r）を、公開鍵Pにより復号する。つまりD｛P，E（S，r）｝の処理を行う。そして処理S7として、上記処理S2で発生させた乱数rと、上記処理S6での復号結果D｛P，E（S，r）｝を比較する。ここで、公開鍵Pと秘密鍵Sが適正な鍵のペアであったとすると、r＝D｛P，E（S，r）｝の結果が得られるはずである。そこで、比較結果が一致していた場合は、当該二次記録媒体側機器20Aが、公開鍵Pに対する秘密鍵Sを保持していることが確認されたことになるため、処理S8から処理S9に進み、当該二次記録媒体側機器20Aを正当な接続相手として認証する。一方、比較結果が一致していなければ処理S8から処理S10に進み、接続された二次記録媒体側機器は、正当な接続相手（即ちSDMIコンテンツを転送してよい機器）ではないとして認証NGとする。

【0143】例えば以上のような認証処理により、接続された機器が、適正な二次記録媒体側機器20Aとして認証されると、一次記録媒体側機器1は、その接続された機器に対してSDMIコンテンツの転送を許可する条件の1つが満たされと認識することになる。

【0144】8．コンテンツ暗号化方式

本例のシステムにおいて、図1に示した構造の最下段のデバイスに相当するのは記録再生装置20A，20Bとなるが、図1に示したような暗号化構造を当該システムにおいて実現する場合の例を説明する。

【0145】まず図13はコンテンツデータ及びキーの流れを示している。図4に示した外部サーバ91からパーソナルコンピュータ1に或るコンテンツデータCT1が配信される場合、この1単位のコンテンツキーCT1については、E（CK，A3D），E（KR，CK）、及びEKBが送信されてHDD5に格納されることになる。E（CK，A3D）はコンテンツキーCKで暗号化されたATRAC3圧縮コンテンツデータであ

り、つまり配信目的たる実際の音楽その他の情報である。E（KR，CK）は、コンテンツデータの暗号解読のためのコンテンツキーCKを、図1で説明したルートキーKRで暗号化した情報である。EKBは図1～図3で説明した有効化キーブロックの情報であり、本実施の形態の説明においては、ルートキーKRを更新するための情報であるとする。

【0146】1つのコンテンツデータの配信に応じて、これらがセットで配信され、図示するようにHDD5には、これらのセットとしてのコンテンツデータCT1，CT2・・・が格納されるものとなる。

【0147】パーソナルコンピュータ1が記録再生装置20A又は20Bに対してコンテンツデータ転送を行う場合は、このセットとしての情報としてE（CK，A3D），E（KR，CK），及びEKBを、所定の手順で送信する。図1で説明したデバイス（端末）に相当する記録再生装置20A、20Bでは、それぞれ固有のリーフIDが設定されており、またDNK（Device Node Key）を記憶している。

【0148】そしてパーソナルコンピュータ1から上記セットのコンテンツデータが送信されてくることに応じて、コンテンツデータの暗号解読を行い（又は暗号化状態のまま）、二次記録媒体に記録する。SDMI対応の記録再生装置20Bの場合は、再生時において暗号解読を行うことになる。また記録再生装置20Aの場合は、記録時において暗号解読を行う。

【0149】この暗号解読の処理としては、図示するように、まず記憶しているDNKと送信されてくるEKBを用いてルートキーKRを解読する。続いて解読したルートキーKRを用いてコンテンツキーCKを解読する。そして解読したコンテンツキーCKを用いることで、暗号化を解除したコンテンツデータA3Dを得ることができる。

【0150】記録再生装置20Aの場合のDNK及び暗号解読手順を図14，図15で具体的に説明する。今、図14（a）のようなキーのツリー構造を想定し、例えば記録再生装置20Aに、リーフID＝SET0、リーフキー＝K000が設定されているとする。この場合、記録再生装置20Aに記憶されるDNKは、図14（b）のような情報を有する。まずリーフIDとして「SET0」が記憶される。またリーフキーとして「K000」が記憶される。そしてリーフキー「K000」から図14（a）の構造でルートキーKRまでをたどることのできる情報が記憶される。つまり、ノードキーK00、K0、ルートキーKRが記憶される。但しこのノードキーK00、K0、ルートキーKRは、リーフキーK000によって暗号化された状態で記憶される。即ち図示するように、

E（K000，K00）

E（K000，K0）

E（K000，KR）

が記憶されるものとなる。

【0151】このようなDNKが記憶されていることで、記録再生装置20Aは、転送されてきたコンテンツデータE（CK，A3D）を、同じく転送されてきたE（KR，CK）を用いて暗号解読できる。即ちこの場合は、記録再生装置20AはリーフキーK000を用いてD{K000，E（K000，KR）}の復号を行うことでルートキーKRを得ることができる。そして復号したルートキーKRを用いてD{KR，E（KR，CK）}の復号を行うことでコンテンツキーCKを得ることができる。さらに復号したコンテンツキーCKを用いてD{CK，E（CK，A3D）}の復号を行うことで暗号解読されたコンテンツデータA3Dを得ることができる。

【0152】但し、上述したように常にルートキーKRやノードキーは不変のものではなく多様な事情により変更される。そしてこの例のようにコンテンツキーCKをルートキーKRで暗号化して転送するシステムの場合は、コンテンツデータ毎にルートキーKRを変更することもあり得る。例えば音楽配信業者によっては1つのコンテンツデータ毎にルートキーKRを変更し、これによって著作権保護を強化する場合がある。このために、上記のようにEKBを同時に送信して、正規のデバイスに対して変更したルートキーKRが確認できるようにしている。

【0153】いま、図15に示すように、或るコンテンツデータE（CK，A3D）について、変更したルートキーKR'で暗号化したコンテンツキーE（KR'，CK），及びEKBが送信されてくるとする。この場合EKBには、例えばノードキーK0で暗号化した更新ルートキーKR'としてE（K0，KR'）の情報が含まれていたとする。なお更新ルートキーKR'をノードキーK0で暗号化することは、例えば図14のデバイス（SET0）～（SET3）のみに対して、新たなルートキーKR'を通知する場合などに行われる例となる。もちろんデバイス（SET0）（SET1）のみを通知対象とするなら、更新ルートキーKR'をノードキーK00で暗号化したE（K00，KR'）の情報が含むEKBを発行すればよい。

【0154】一方、記録再生装置20AのDNKは、図14（b）で説明したように、リーフキーK000と、リーフキーで暗号化されたノードキー及びルートキーとしてE（K000，K00），E（K000，K0），E（K000，KR）が記憶されている。この状態において、コンテンツデータA3Dを復号するまでの手順を図15に①～④で示している。

【0155】① EKBとしてE（K0，KR'）の情報が送られてきたことに応じて、まずDNKからK0を得る。即ちリーフキーK000を用いてD{K000，

Ｅ（Ｋ０００，Ｋ０）｝の復号を行うことでノードキーＫ０を得る。

② 次にノードキーＫ０を用いて、ＥＫＢによるＥ（Ｋ０，ＫＲ’）を解読する。即ちＤ｛Ｋ０，Ｅ（Ｋ０，ＫＲ’）｝の復号を行うことで更新ルートキーＫＲ’を得る。

③ 解読した更新ルートキーＫＲ’を用いて、送信されてきたコンテンツキーＥ（ＫＲ’，ＣＫ）を解読する。つまりＤ｛ＫＲ’，Ｅ（ＫＲ，ＣＫ）｝の復号を行うことでコンテンツキーＣＫを得る。

④ 復号したコンテンツキーＣＫを用いてＤ｛ＣＫ，Ｅ（ＣＫ，Ａ３Ｄ）｝の復号を行うことで暗号解読されたコンテンツデータＡ３Ｄを得る。

【０１５６】以上の手順により、記録再生装置２０Ａでは、転送されてきたコンテンツデータの暗号化を解除して、ミニディスク１００に記録することができる。また記録再生装置２０Ｂの場合では、暗号化された状態で二次記録媒体に記録したコンテンツデータを再生する際に、上記手順によって暗号化を解除し、音楽等の再生を行うことができる。

【０１５７】９．各種コマンド

一次記録媒体側機器であるパーソナルコンピュータ１と、二次記録媒体側機器である記録再生装置２０Ａ（２０Ｂ）との間では、チェックアウト／チェックイン或いは他の各種の動作のための通信セッションにおいて、各種のコントロールコマンド及びそれに対するレスポンスコマンドのやりとりが行われる。ここでは、多様なコマンドのうち、後述する本例の特徴的な動作に直接的に関連するコマンドのみについて、説明しておく。

【０１５８】図１６にチェックアウトコントロールコマンド、図１７にチェックアウトレスポンスコマンドの各フォーマットを示す。チェックアウトコントロールコマンドは２５バイトで構成され、チェックアウトレスポンスコマンドは１７バイトで構成される。そしてチェックアウトコントロールコマンドは、チェックアウトのための通信セッションにより二次記録媒体側に転送したコンテンツデータを、実際に二次記録媒体側が再生可能な状態とすること（再生権を与える）を指示するために、パーソナルコンピュータ１が記録再生装置２０Ａ（２０Ｂ）に対して発するコマンドとなる。一方、記録再生装置２０Ａ（２０Ｂ）は、これに対応して所定の処理を行い、コントロールコマンドに対する応答としてチェックアウトレスポンスコマンドをパーソナルコンピュータ１に送信する。

【０１５９】図１６に示すようにチェックアウトコントロールコマンドでは、オペレーションコードとして「チェックアウト」が示され、通信結果（result）、通信対象機器の識別コード（List ID）、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ（object position number）、暗号化セッションキー（DES CBC(Ks,0)）としての各情報ビットが用意される。またチェックアウトレスポンスコマンドは、図１７に示すように、オペレーションコードとして「チェックアウト」が示され、通信結果（result）、通信対象機器の識別コード（List ID）、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ（object position number）としての各情報ビットが用意される。

【０１６０】図１８に３０バイトとされるレコードオブジェクトコントロールコマンド、図１９に６２バイトのレコードオブジェクトレスポンスコマンドの各フォーマットを示す。レコードオブジェクトコントロールコマンドは、例えばチェックアウトのための通信セッションにおいて、実際のコンテンツデータの転送に際してそのコンテンツデータの情報を通知するためなどに、パーソナルコンピュータ１が記録再生装置２０Ａ（２０Ｂ）に対して発するコマンドとなる。一方、記録再生装置２０Ａ（２０Ｂ）は、これに対応して通知された情報等に関する処理を行い、コントロールコマンドに対する応答としてチェックアウトレスポンスコマンドをパーソナルコンピュータ１に送信する。また後述するが、記録再生装置２０Ａにおいては、転送されてくるコンテンツデータの一部を用いてコンテンツＩＤを生成するが、レコードオブジェクトレスポンスコマンドにより、当該生成したコンテンツＩＤをパーソナルコンピュータ１に通知することも行う。

【０１６１】図１８に示すようにレコードオブジェクトコントロールコマンドでは、オペレーションコードとして「レコードオブジェクト」が示され、通信結果（result）、通信対象機器の識別コード（Destination List ID）、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ（new object position number）、コンテンツデータのタイプ（content type）、一次記録媒体側のコンテンツデータフォーマット（Download Format Track Attribute）、二次記録媒体におけるコンテンツ属性（Track Mode）、コンテンツデータのデータ長（ContentSize）、コンテンツデータのバルクデータ長（Bulk Data Size）としての各情報ビットが用意される。一次記録媒体側のコンテンツデータフォーマット（Download Format Track Attribute）とは、ＨＤＤ５に格納されている、送信しようとするコンテンツデータの圧縮方式及びビットレートの情報や、コンテンツデータを伝送路に送出する際のコンテンツデータの圧縮方式及びビットレートの情報である。二次記録媒体におけるコンテンツ属性（Track Mode）とは、ミニディスク１００へ記録する際の圧縮方式の指定情報や、ステレオ・モノラルその他の属性情報である。圧縮方式としては、例えばＡＴＲＡＣ、ＡＴＲＡＣ３の１３２ｋｂｐｓ、ＡＴＲＡＣ３の６６ｋｂｐｓのいずれかが指定される。

【０１６２】これと同様に図１９に示すレコードオブジ

ェクトレスポンスコマンドは、オペレーションコードとして「レコードオブジェクト」が示され、通信結果（result）、通信対象機器の識別コード（Destination List ID）、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ（new object position number）、コンテンツデータのタイプ（content type）、一次記録媒体側のコンテンツデータフォーマット（Download Format Track Attribute）、二次記録媒体におけるコンテンツ属性（Track Mode）、コンテンツデータのデータ長（Content Size）、コンテンツデータのバルクデータ長（Bulk Data Size）としての各情報ビットが用意される。そしてさらにレスポンスコマンドの場合は、３２バイトのセッションデータとして、記録再生装置２０Ａにおいて算出されたコンテンツＩＤの情報をパーソナルコンピュータ１に通知する領域が用意されている。コンテンツＩＤについては後に詳述する。

【０１６３】図２０にチェックインコントロールコマンド、図２２にチェックインレスポンスコマンドの各フォーマットを示す。チェックインコントロールコマンドは１７バイトで構成され、チェックインレスポンスコマンドは２５バイトで構成される。そしてチェックインコントロールコマンドは、通信セッションにより二次記録媒体側のコンテンツデータをチェックインさせる、つまり二次記録媒体側での再再生権を返却させることを指示するために、パーソナルコンピュータ１が記録再生装置２０Ａ（２０Ｂ）に対して発するコマンドとなる。ただし、チェックイン以外にパーソナルコンピュータ１が二次記録媒体側の固有情報を得るために発する場合もある。一方、記録再生装置２０Ａ（２０Ｂ）は、チェックインコントロールコマンドに対応して所定の処理を行い、コントロールコマンドに対する応答としてチェックインレスポンスコマンドをパーソナルコンピュータ１に送信する。

【０１６４】図２０に示すようにチェックインコントロールコマンドでは、オペレーションコードとして「チェックイン」が示され、通信結果（result）、サブファンクション（Subfunction）、通信対象機器の識別コード（List ID）、チェックインコンテンツについての二次記録媒体側でのトラックナンバ（object position number）としての各情報ビットが用意される。

【０１６５】ここで、サブファンクションは図２１のように定義され、これによってチェックインコマンドによる指示内容が指定される。サブファンクションの値が「００ｈ」であれば、そのチェックインコントロールコマンドは、コンテンツＩＤを要求するものとなる。これは二次記録媒体側の再生権を返却させる実際のチェックインとしての指示となる。サブファンクションの値「０１ｈ」はリザーブとされる。但し実際のチェックイン処理過程における指示に用いてもよい。サブファンクションの値がそれら以外の場合は、そのチェックインコントロールコマンドは、プリペイド情報を要求するものとなる。プリペイド情報については後述するが、これは二次記録媒体に記録された固有情報の一つである。そして、この場合は、チェックインコントロールコマンドは、あくまでプリペイド情報の読出を指示するものであって、チェックイン（再生権の返却）は行われない。なお、プリペイド情報以外に、二次記録媒体側の固有情報、例えばユーザー情報や使用状況などの情報等を要求できるようにサブファンクションの値を定義することもできる。

【０１６６】またチェックインレスポンスコマンドは、図２２に示すように、オペレーションコードとして「チェックイン」が示され、通信結果（result）、サブファンクション（Subfunction）、通信対象機器の識別コード（List ID）、チェックインコンテンツについての二次記録媒体側でのトラックナンバ（object position number）としての各情報ビットが用意される。そして更にHASH関数処理で形成されたコンテンツＩＤをパーソナルコンピュータ１側に通知するための８バイト（Hash MAC）が用意される。但し、この最後の８バイトにコンテンツＩＤが組み込まれて通信されるのは、上記チェックインコントロールコマンドとしてサブファンクションの値が「００ｈ」であった場合、つまり実際にチェックインが行われる場合である。

【０１６７】チェックインコントロールコマンドのサブファンクションの値によりプリペイド情報が要求された場合は、図２３のように最後の８バイトにおいてプリペイド情報が組み込まれて、パーソナルコンピュータ１に対して送信されることになる。

【０１６８】図２４はイクスクルーシブログインコントロールコマンド、図２５はイクスクルーシブログアウトコントロールコマンドを示している。このコマンドは、パーソナルコンピュータ１が記録再生装置２０Ａに対して排他的制御を行うためのコマンドである。イクスクルーシブログインコントロールコマンドでは、サブユニットタイプ（subunit type）、サブユニットＩＤ（subunit ID）により制御対象機器が示される。そしてプライオリティ（priorty）の値により、制御レベルが指示される。なお、イクスクルーシブログアウトコントロールコマンドは、記録再生装置２０Ａに対する排他的制御を解除するためのコマンドであり、この場合はプライオリティ（priorty）の値を「００ｈ」とし、フリー状態の制御レベルであることを指示するコマンドとして形成されている。

【０１６９】イクスクルーシブログインコントロールコマンドにより、記録再生装置２０Ａは二次記録媒体（ミニディスク１００）に対するコンテンツデータの消去、編集、或いはディスク排出、電源制御などが禁止又は制限される。つまりこのコマンドは、これらの動作処理はあくまでもパーソナルコンピュータ１側から指示されるものとする状態に遷移させるコマンドである。

【0170】このイクスクルーシブログインコントロールコマンドによるプライオリティの値によっては、動作の禁止又は制限として多様な状態を設定できる。例えば、記録再生装置２０Ａに対して、

制御レベル４：パーソナルコンピュータ１以外の一切の指示に対応する処理を禁止する。

制御レベル３：パーソナルコンピュータ１以外の指示による電源制御、イジェクト、トラックの分割、連結、消去を禁止する。

制御レベル２：パーソナルコンピュータ１以外の指示によるトラックの分割、連結、消去を禁止する。

制御レベル１：チェックアウトコンテンツではないトラックについては編集や消去を許可する。

制御レベル０：制限無し

などのように各種状態を設定できる。もちろん、このような制御レベルの設定は一例であり、実際には制御レベルの段階数や内容は多様に考えられる。

【0171】１０．コンテンツのチェックアウト／チェックイン

続いてパーソナルコンピュータ１のＨＤＤ５に格納されたコンテンツデータを記録再生装置２０Ａにチェックアウトさせる場合、及びチェックアウトさせたコンテンツデータをチェックインさせる場合のそれぞれについて、パーソナルコンピュータ１と記録再生装置２０Ａで行われる処理を説明する。なお、実際には１つの通信セッションで複数のコンテンツデータのチェックアウト／チェックインが行われることも多いが、説明の簡略化のため、１つのコンテンツデータのチェックアウト／チェックインとしての処理の流れを説明することとする。

【0172】図２６，図２７はチェックアウトのための処理を示している。図２６，図２７において、パーソナルコンピュータ１のＣＰＵ２が実行する制御処理をステップＦ１０１～Ｆ１１１とし、また記録再生装置２０Ａのシステム制御部３２、復号処理部２８等によって実行される制御処理をステップＦ２０１～Ｆ２１５として示している。なお、通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【0173】ＨＤＤ５に格納されている或るコンテンツデータの転送を行う場合は、ＣＰＵ２は図２６のステップＦ１０１として記録再生装置２０Ａに対して認証処理の開始を要求する。即ち認証開始コントロールコマンドを送信する。これに対して記録再生装置２０Ａはパーソナルコンピュータ１に対してステップＦ２０１で認証開始許可を通知する。即ち認証開始レスポンスコマンドを送信する。

【0174】するとパーソナルコンピュータ１はステップＦ１０２としてリーフＩＤを要求し、これに応じて記録再生装置２０Ａはステップ２０２で記憶しているリーフＩＤを送信する。なお、パーソナルコンピュータ１は接続された記録再生装置２０Ａを、このようにリーフＩＤを確認して、現在有効なリーフＩＤの機器であるか否かを確認する。

【0175】続いて、パーソナルコンピュータ１はステップＦ１０３として、これから転送しようとするコンテンツデータについてのＥＫＢを記録再生装置２０Ａに送信する。記録再生装置２０Ａでは、ＥＫＢが送信されてきたら、まずステップＦ２０３でＥＫＢのバージョンナンバを記憶する（図３参照）。さらにステップＦ２０４で、受信したＥＫＢと、記憶しているＤＮＫを用いて、図１５で説明した手順①②のようにして、今回の転送にかかるコンテンツデータのルートキーＫＲを探索し、得られたルートキーＫＲを記憶する。そしてステップＦ２０５で、ルートキーＫＲの探索完了をパーソナルコンピュータ１側に通知する。

【0176】以上の処理でルートキーＫＲの確認が完了したことから、パーソナルコンピュータ１はステップＦ１０４として、実際のチェックアウトセッションの開始を要求する。これに対して、記録再生装置２０Ａはステップ２０６でチェックアウトセッションの開始を了承する通知を行う。なお、このセッション開始のコントロールコマンド及びレスポンスコマンドの際には、図１２で説明した認証処理も行われることになる。つまり、ＳＤＭＩ非対応であって、暗号化を解いてコンテンツデータを二次記録媒体に記録する記録再生装置２０Ａとして、正規なものであるか否かの認証が行われる。図２６には示していないが、もちろん認証ＮＧとなればチェックアウトセッションは中止される。

【0177】次にパーソナルコンピュータ１はステップＦ１０５で、今回転送しようとするコンテンツデータに係る、暗号化コンテンツキーＥ（ＫＲ，ＣＫ）を送信する。これを受けた記録再生装置２０Ａではステップ２０７で上記図１５の手順③のように、記憶したルートキーＫＲを用いて、暗号化コンテンツキーＥ（ＫＲ，ＣＫ）を復号し、コンテンツキーＣＫを解読する。そしてステップＦ２０８で、パーソナルコンピュータ１に対してコンテンツキーＣＫの解読完了を通知する。

【0178】続いてパーソナルコンピュータ１はステップＦ１０６で、図１８により説明したレコードオブジェクトコントロールコマンドを送信し、記録再生装置２０Ａに対して、チェックアウトしようとするコンテンツの情報を提供する。なお、図示していないが、これに対して記録再生装置２０Ａはレスポンスコマンドを返す。（この場合のレスポンスコマンドは図１９の形式ではなく、図示及び説明を省略した２５バイトの形式である。）

【0179】そしてコンテンツキーＣＫの解読完了通知及びレコードオブジェクトコントロールコマンドに対するレスポンスにより、パーソナルコンピュータ１は記録再生装置２０Ａ側でコンテンツデータ受信／解読のため

の準備が完了したことを認識できるため、次に「Ｐ１」として示すように図２７のステップＦ１０７に進み、コンテンツデータの転送を実行する。即ちコンテンツキーＣＫで暗号化されたコンテンツデータＥ（ＣＫ，Ａ３Ｄ）を送信する。記録再生装置２０Ａ側では「Ｒ１」で示すように図２７のステップＦ２０９に進み、送信されてきたコンテンツデータＥ（ＣＫ，Ａ３Ｄ）の受信処理、図１５の手順④のようにコンテンツキーＣＫを用いた復号処理、及び復号されたコンテンツデータＡ３Ｄのミニディスク１００への記録処理を行うことになる。さらに、詳しくは後述するが、受信され非暗号化状態に復号したコンテンツデータから、コンテンツＩＤを生成する処理も行う。

【０１８０】１つのコンテンツデータ（例えば１つの楽曲）について、パーソナルコンピュータ１からの転送及びミニディスク１００への記録が完了したら、その時点でミニディスク１００上のＵ－ＴＯＣの更新が必要になる。ミニディスク１００では、上述したように例えば１曲の単位としてのトラックのスタートアドレス／エンドアドレスその他を、ディスク内周部に記録されるＵ－ＴＯＣにおいて管理するものであり、トラックの再生時にはＵ－ＴＯＣからディスク上のアドレスを把握するものであるためである。

【０１８１】但し本例では、１つのコンテンツデータについてのミニディスク１００への記録が終了した時点では、ステップＦ２１０として示すように、バッファメモリ３０上でＵ－ＴＯＣを更新するのみにとどめ、ミニディスク１００上でＵ－ＴＯＣを更新することは行わない。そして、バッファメモリ３０上でＵ－ＴＯＣ更新を完了したら、ステップＦ２１１でパーソナルコンピュータ１に対して、図１９で説明したレコードオブジェクトレスポンスコマンドを送信する。これにより、１つのコンテンツデータの書込に関する処理を完了し、かつ、そのコンテンツデータについてステップＦ２０９の際に生成したコンテンツＩＤをパーソナルコンピュータ１に通知する。

【０１８２】パーソナルコンピュータ１側では、コンテンツＩＤの通知に応じて、ステップＦ１０８としてコンテンツＩＤテーブルの処理を行う。これについては後述するが、これはＨＤＤらに蓄積されたコンテンツデータに対応してパーソナルコンピュータ１側で付したコンテンツＩＤと、上記のステップＦ２０９における処理において記録再生装置２０Ａ側で生成されたコンテンツＩＤを対応させる処理となる。

【０１８３】次にパーソナルコンピュータ１は、ステップＦ１０９として、図１７に示したチェックアウトコントロールコマンドを送信する。またパーソナルコンピュータ１は、このようにチェックアウトを行なうことに応じて、ステップＦ１１０で、当該コンテンツデータに関して扱いルール（Usage Rule）を更新する。即ち転送許可回数としてのコンテンツ権利を１つ減算する。

【０１８４】記録再生装置２０Ａ側では、チェックアウトコントロールコマンドによりチェックアウトが実際に指示されたとして処理を行う。即ちステップＦ２１２で、ミニディスク１００上でＵ－ＴＯＣを更新し、記録したコンテンツデータを再生可能な状態とする。これにより二次記録媒体上でコンテンツデータの再生権が与えられたことになる。なお、このとき、当該コンテンツデータに対応するＵ－ＴＯＣセクター０のトラックモードにおいて、上述したビットｄ１＝１とされており、つまり当該コンテンツデータはライトプロテクト状態とされる。そして、記録再生装置２０Ａは、チェックアウトにかかるＵ－ＴＯＣ更新を終了することに応じて、ステップＦ２１３でチェックアウトレスポンスコマンドを送信し、完了を通知する。以上でチェックアウト、つまりコンテンツ権利の譲渡が完了する。

【０１８５】チェックアウトの完了に応じて、パーソナルコンピュータ１はステップＦ１１１でセッション終了要求のコントロールコマンドを記録再生装置２０Ａに送信する。記録再生装置２０Ａはステップ Ｆ２１４としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ１に送信する。またパーソナルコンピュータ１はステップＦ１１２で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置２０Ａはステップ Ｆ２１５で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、チェックアウトのための一連の通信が終了される。

【０１８６】なお、このような通信により複数のコンテンツデータをチェックアウトする場合は、各コンテンツについてルートキーが共通であれば、ステップＦ１０５～Ｆ１０８及びＦ２０７～Ｆ２１１の処理が繰り返されればよい。またＥＫＢバージョンが異なるコンテンツデータを連続して転送する場合は、コンテンツに対応してＥＫＢ転送も行えばよい。

【０１８７】続いてチェックインの場合の処理を図２８で説明する。図２８において、パーソナルコンピュータ１のＣＰＵ２が実行する制御処理をステップＦ１０１～Ｆ１５６とし、また記録再生装置２０Ａのシステム制御部３２、復号処理部２８等によって実行される制御処理をステップＦ２０１～Ｆ２５７として示している。この場合も、通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【０１８８】チェックインの場合も、認証開始からＥＫＢ転送、ルートキー探索等の処理は上記チェックアウトの場合と同様に行われる。即ち上記図２６と同一のステップ番号を付したステップＦ１０１～Ｆ１０３、Ｆ２０１～Ｆ２０５は、上述と同様の処理が行われるものであり、重複説明を避ける。

【０１８９】パーソナルコンピュータ１はステップＦ１５０で、チェックインセッションの開始を要求するコン

トロールコマンドを送信する。これに応じて記録再生装置２０Ａはステップ Ｆ２５０で、レスポンスコマンドを返す。なお、この場合にも、図１２で説明した認証処理が行われる。

【０１９０】チェックインセッションが開始され、且つ記録再生装置２０Ａが認証ＯＫとなったら、パーソナルコンピュータ１はステップＦ１５１として、チェックインさせようとするコンテンツデータについてのコンテンツＩＤを要求する。例えば記録再生装置２０Ａに対してチェックインさせるコンテンツデータのミニディスク１００上のトラックナンバを指定して、そのコンテンツＩＤを要求する。記録再生装置２０Ａは、これに応じて、まずステップＦ２５１で、当該指定されたコンテンツデータ（トラック）が、チェックイン可能なコンテンツデータであるか否かを判断する。この判断はトラックに対応してＵ－ＴＯＣに記録されている書込制御フラグの状態（トラックモードのｄ１）で判別できる。これについては後述する。ここで判断するチェックイン可能なコンテンツデータとは、チェックアウトされたコンテンツデータであって、しかもミニディスク１００側で編集が行われていないコンテンツデータである。

【０１９１】チェックイン可能なコンテンツデータであれば、ステップＦ２５２で、当該コンテンツデータについてのコンテンツＩＤを用意する。この場合、この時点でコンテンツＩＤを算出するか、或いは既に算出されて記憶されているコンテンツＩＤを読み出す処理となる。これについても後述する。そしてステップＦ２５３で、コンテンツＩＤをパーソナルコンピュータ１に送信する。なお、チェックイン可能なコンテンツデータでなかった場合は、その旨をパーソナルコンピュータ１に通知し、以降はエラー処理となる。

【０１９２】パーソナルコンピュータ１はステップＦ１５２として、送信されてきたコンテンツＩＤを照合する。つまり、記録再生装置２０Ａ側で生成され送信されてきたコンテンツＩＤと、チェックアウト時に記録再生装置２０Ａ側で生成し、パーソナルコンピュータ１側で生成したコンテンツＩＤに対応させてテーブルデータとして保存したコンテンツＩＤの照合をとり、チェックイン対象のコンテンツデータを正しく示しているかを照合する。そして照合ＯＫであればステップＦ１５３で実際にチェックインを指示する。照合ＮＧであればエラー処理となる。

【０１９３】ステップＦ１５３のチェックイン指示は、図２０で説明したチェックインコントロールコマンドを送信するものとなる。このときチェックインコントロールコマンドにおいては、サブファンクションの値は「００ｈ」とし（図２１参照）、これによって実際のチェックイン指示であることを明示する。またリストＩＤの値を記録再生装置２０Ａを指定した値とし、オブジェクトポジションナンバの値として、チェックインさせるコンテンツデータのミニディスク１００上のトラックナンバを指定するものとなる。また、チェックイン指示に応じてステップＦ１５４で、当該コンテンツデータについての扱いルール（Usage Rule）を更新する。即ち転送許可回数としてのコンテンツ権利を１つ復活させる。

【０１９４】記録再生装置２０Ａ側は、これに応じてステップＦ２５４で、Ｕ－ＴＯＣデータを更新する。つまりチェックイン対象となったトラックを、ミニディスク１００上から消去されるようにＵ－ＴＯＣセクター０の内容を更新する。つまり再生不能とし、再生権を消失した状態とする。そしてステップＦ２５５で図２２のチェックインレスポンスコマンドを送信する。以上でチェックイン、つまりコンテンツ権利の返却が完了する。

【０１９５】チェックインの完了に応じて、パーソナルコンピュータ１はステップＦ１５５でセッション終了要求のコントロールコマンドを記録再生装置２０Ａに送信する。記録再生装置２０ＡはステップＦ２５６としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ１に送信する。またパーソナルコンピュータ１はステップＦ１５６で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置２０Ａはステップ Ｆ２５７で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、チェックインのための一連の通信が終了される。

【０１９６】なお、このような通信により複数のコンテンツデータをチェックインする場合は、各コンテンツＩＤの確認及びチェックイン指示、つまりステップＦ１５１～Ｆ１５４及びＦ２５１～Ｆ２５５の処理が繰り返されればよい。

【０１９７】１１．コンテンツＩＤの生成及び管理方式
チェックアウト／チェックインにおけるUsage Rule
は、各コンテンツ毎にコンテンツＩＤを用いて管理される。上述したが、ＳＤＭＩ対応の二次記録媒体では、コンテンツＩＤが格納できる記録フォーマットが採られている。従って、チェックアウト／チェックインの際も、パーソナルコンピュータ１とＳＤＭＩ対応の記録再生装置２０Ｂの間では、元々パーソナルコンピュータ１側で生成したコンテンツＩＤにより、対象となっているコンテンツデータを特定できる。

【０１９８】しかしながら、従来より普及しているミニディスク１００等の二次記録媒体を対象とする、記録再生装置２０Ａでは、これができない。つまりミニディスク１００上には、チェックアウトにより記録されたコンテンツデータについてのコンテンツＩＤを格納しておく領域が存在しないためである。仮にＵ－ＴＯＣなどにおいてそのような領域を新たに規定しコンテンツＩＤを記録したとしても、従前の機種のミニディスクレコーダによってＵ－ＴＯＣ更新が行われた場合、コンテンツＩＤは消去されてしまう。このためミニディスク１００では コンテンツＩＤを管理できない。二次記録媒体側でコン

テンツＩＤが管理できなければ、チェックアウトは可能でもチェックインの際にはコンテンツデータの照合がとれないため、チェックイン不能となる。

【０１９９】そこで記録再生装置２０Ａでは、コンテンツデータ自体からコンテンツＩＤを生成する機能を備えるようにする。そしてパーソナルコンピュータ１側では、パーソナルコンピュータ１側で発生させた第１のコンテンツＩＤと、記録再生装置２０Ａ側で生成した第２のコンテンツＩＤを照合できるようにテーブルデータを用意するものとしている。

【０２００】まず、記録再生装置２０Ａによりコンテンツ ＩＤを生成する方式を説明する。コンテンツＩＤ生成においては、非暗号化状態に復号されたコンテンツデータについて、そのコンテンツデータの長さ（コンテンツサイズ）やトラック情報に加えて、コンテンツデータストリーム内の特定のデータをサンプリングしてＣＢＣ＿ＭＡＣ演算をする手段などがあげられる。

【０２０１】図２９に、１つの音楽等のコンテンツデータの全体を模式的に示している。このコンテンツデータは、例えばパーソナルコンピュータ１からチェックアウトにために送信され、暗号化状態が復号され、ＡＴＲＡＣ又はＡＴＲＡＣ３圧縮状態のデータストリームとして示している。このコンテンツデータに対して、例えばポイントＰ１，Ｐ２をサンプリングポイントとして設定し、サウンドユニット（斜線部）のデータを抽出する。１つのサウンドユニットは、例えば４２４バイトのデータ、つまり図８で説明した１つのサウンドグループに相当するデータなどとすればよい。ただしもちろんそれに限定されない。

【０２０２】そして、このようにサンプリングした実際のコンテンツデータの一部を用いてコンテンツＩＤを算出する。ここで、サンプリングポイントは、無音データであることが多いことが予想されるコンテンツの先頭又は終端は避けるとともに、上記Ｐ１，Ｐ２のように２箇所設けることでユニークデータとしての確率を高めることができる。つまり各コンテンツデータ毎に異なる、識別子としての機能を十分に備えたコンテンツＩＤを算出できる。もちろんサンプリングポイントは３カ所以上としてもよい。また先頭又は終端を避ければ、１カ所であっても不十分ではない。

【０２０３】また、このサンプリングポイントＰ１，Ｐ２は、全くランダムな位置ではなく、コンテンツデータのレングス（データサイズ）に応じて設定される位置とすることで、特定のコンテンツデータについては、何度算出しても同じコンテンツＩＤが得られる。つまり、二次記録媒体上においてコンテンツＩＤを保存しておかなくてもコンテンツデータ自体が記録されていれば、サンプリングポイントが一致することで異なる時点でも同じコンテンツＩＤが算出できるものであり、このことは、二次記録媒体としてのミニディスク１００上にコンテンツＩＤを記録しておく必要をなくすことができるものとなる。具体的にはサンプリングポイントＰ１，Ｐ２は、例えばコンテンツデータのサイズ（レングス）から１／３の位置、及び２／３の位置などとして設定されればよい。もちろん１／３の位置，２／３の位置に限らず、レングスに対して１／２の位置、１／４の位置、３／４の位置、１／５の位置、２／５の位置、３／５の位置、４／５の位置、１／６の位置、５／６の位置・・・・など、レングスに対する或る相対的なポイントが規定されればよい。

【０２０４】コンテンツデータからハッシュ関数を用いてコンテンツＩＤを得る方法を下記（１）式に示す。

Content ID=CBC_MAC (Key hash, IV, Stream(P1)//Stream(P2))・・・（１）

ここで「Key hash」は８バイトの固有鍵データである。Stream(P1)は、サンプリングポイントＰ１の１サウンドグループのデータ、Stream(P2)は、サンプリングポイントＰ２の１サウンドグループのデータである。そして／／は連結を示しており、つまり「Stream(P1)//Stream(P2)」は、サンプリングポイントＰ１，Ｐ２の２つのサウンドユニットを繋げた（４２４×２）バイトのデータを示している。また「IV」は８バイトのＣＢＣモードの初期値であり、４バイトのコンテンツ長length、１バイトのトラック情報TrackModeByteを用いて次の（２）式で与えられる。

IV={length//TrackModeByte//32bits Padding with Zero}　・・・（２）

この場合、４バイトのコンテンツ長length、及び１バイトのトラック情報TrackModeByteは、図１８に示したレコードオブジェクトコントロールコマンドによって通知される、４バイトのコンテンツサイズ（Content Size）と１バイトのトラックモード（Track Mode）の情報を用いることができる。

【０２０５】このようなコンテンツＩＤ生成は、記録再生装置２０Ａにおいて例えば復号処理部２８に搭載されるHASHエンジンによって行われるが、上記式（１）（２）からわかるように、記録再生装置２０Ａは、例えばチェックアウトセッションの際には、レコードオブジェクトコントロールコマンドを受信（図２６のステップＦ１０６）することで、上記「IV」の値を算出できる。またレコードオブジェクトコントロールコマンドにおけるコンテンツサイズ（Content Size）によりコンテンツデータが転送される前に、コンテンツデータのレングスが確認できるため、コンテンツデータのレングスの例えば１／３，２／３の位置としてのサンプリングポイントＰ１，Ｐ２も確認できる。従って、実際にコンテンツデータの転送が開始され、サンプリングポイントＰ１，Ｐ２のデータが得られた時点以降は、上記式（１）の演算によりコンテンツＩＤを算出できるものである。

【0206】また、ミニディスク100上に記録されたコンテンツデータについては、当然ながらコンテンツデータのサイズはU-TOCセクター0のデータから算出できるため、サンプリングポイントP1，P2の位置は確認できる。またチェックアウト時にレコードオブジェクトコントロールコマンドで通知されるトラックモード（Track Mode）の情報が、U-TOCセクター0におけるトラックモードに記録されることで、U-TOCデータから上記式（2）の算出が可能となる。従って、ミニディスク100上に記録されたコンテンツデータについては、どのような時点でもコンテンツIDを算出できるものとなる。

【0207】例えばこのようにして、記録再生装置20A側ではチェックアウトされたコンテンツデータについて独自にコンテンツIDを生成することができる。ただし、これがパーソナルコンピュータ1において生成され、HDD5に格納されたコンテンツIDと対応づけられなければ適切に利用できない。上述したようにHDD5に格納されるコンテンツIDとは、パーソナルコンピュータ1側のアプリケーションにより、コンテンツデータについて生成されたものである。このアプリケーションによって予め求められたコンテンツIDは、HDD5などの一次記録媒体を有する機器側（パーソナルコンピュータ1）に固有な情報、例えば機器にインストールされたアプリケーション毎のユニークID、HDD5に格納された時間情報や乱数などで構成される。このようなパーソナルコンピュータ1側で生成された（第1の）コンテンツIDと、上記記録再生装置20A側で生成された（第2の）コンテンツIDは、図30のようなテーブルデータにより、パーソナルコンピュータ1側で対応づけられる。なお従って、該テーブルデータは、HDD5などの一次記録媒体を有する機器毎にユニークな組み合わせになる。

【0208】即ちチェックアウトセッションの際には、図27のステップF211としてのレコードオブジェクトレスポンスコマンドにより、記録再生装置20A側で生成したコンテンツIDをパーソナルコンピュータ1側に通知する。そしてステップF108として、パーソナルコンピュータ1側ではテーブルデータの処理を行う。この処理は、即ちチェックアウトのために転送するコンテンツデータについて、パーソナルコンピュータ1側のコンテンツIDと、当該コンテンツデータについて記録再生装置20A側で生成されたコンテンツIDを対応するように、図30のテーブルデータのエレメントを生成していく処理である。図30では3つのコンテンツデータについて、それぞれ第1，第2のコンテンツIDが対応づけられた状態を例示している。

【0209】このようなテーブルデータがパーソナルコンピュータ1側で管理される（例えばHDD5において記録／更新されていく）ことで、ミニディスク100に対してチェックアウトされたコンテンツデータを、コンテンツIDで管理することが可能となり、即ちチェックアウト／チェックインの管理が可能となる。上記のようにミニディスク100上にはコンテンツIDを格納する領域が存在しないが、記録再生装置20A側ではミニディスク100に記録されているコンテンツデータについてはコンテンツIDを算出できる。

【0210】従ってパーソナルコンピュータ1が或るコンテンツデータをチェックインさせない場合は、対象となるコンテンツデータについての（第2の）コンテンツIDを記録再生装置20Aに要求し、送信されてきた（第2の）コンテンツIDと、図30のテーブルデータに記憶されいる（チェックアウト時に記録再生装置20A側から送信されてきた第2の）コンテンツIDとの一致を確認することで、パーソナルコンピュータ1側で（第1の）コンテンツIDで管理しているコンテンツデータのチェックイン処理ができるものとなる。これが図28のステップF151，F152、F252、F253の処理の意味である。

【0211】このようなコンテンツID管理方式により、SDMI非対応の二次記録媒体（ミニディスク100等）に対しても、本システムにおいて適切にチェックアウト／チェックインの管理、つまりコンテンツ権利の管理が可能となる。

【0212】12．チェックアウト時及びチェックイン前のコンテンツIDの生成処理

ところで、記録再生装置20A側でコンテンツIDを生成する必要がある場合とは、通常、チェックアウトに応じてコンテンツIDをパーソナルコンピュータ1に通知する場合（パーソナルコンピュータ1側で図30のテーブルデータ管理を行うようにするためにレコードオブジェクトレスポンスコマンドで送信する場合）と、チェックイン等のためにパーソナルコンピュータ1からコンテンツIDを要求された場合となる。

【0213】そして上記のようにコンテンツIDは、サンプリングポイントP1，P2で抽出したコンテンツデータの一部を用いる。このため、例えばチェックアウト時には、パーソナルコンピュータ1から転送されたコンテンツデータがミニディスク100に書き込まれた後において、サンプリングポイントP1，P2のデータを読み出し、そのデータを用いてコンテンツIDを算出するという手順が通常考えられる。またチェックインのためにパーソナルコンピュータ1からコンテンツIDを要求された場合も、その要求に応じてミニディスク100からサンプリングポイントP1，P2のデータを読み出し、そのデータを用いてコンテンツIDを算出するという手順が通常考えられる。

【0214】ただし、このような手順では、チェックアウトセッションの間にミニディスク100に対するアクセス／データ読み出しが必要となり、その分、コンテン

ツＩＤ算出に時間を要する。これはチェックアウトのための全体の通信時間を長時間化するものとなる。またチェックインのためにコンテンツＩＤが要求された際にも、ミニディスク１００に対するアクセス／データ読み出しが必要となり、その分、コンテンツＩＤ算出に時間を要する。これもチェックインのための通信時間を長時間化させる。そこで本例では、次のような手順でコンテンツＩＤ算出を行うことで処理の効率化及び通信時間の短縮をはかる。

【０２１５】図３１はチェックアウトセッションにおけるコンテンツＩＤ（ＣＩＤ）の生成にかかる処理を示している。これは図２７のステップＦ２０９においてシステム制御部３２及び復号処理部２８で行なわれる処理である。図２６のステップＦ１０６として示したように、コンテンツデータの転送直前にパーソナルコンピュータ１からレコードオブジェクトコントロールコマンドが送信されてくるが、図２７のステップＦ２０９における図３１のコンテンツＩＤ生成処理としては、まずステップＦ３０１として、受信したレコードオブジェクトコントロールコマンドの内容から、これから転送されてくるコンテンツデータのレングス（データサイズ）を確認する。そしてステップＦ３０２で、コンテンツデータのレングスから、コンテンツデータストリーム内におけるサンプリングポイントＰ１，Ｐ２としてのポイントを算出する。

【０２１６】ステップＦ３０３は実際に転送されてくるコンテンツデータの受信にかかる処理の開始を示している。即ち図７のブロック図において説明したように、コンテンツデータが受信され、非暗号化状態に復号され、ＡＴＲＡＣ３データ状態でバッファメモリ３０に蓄積され、さらにエンコード／デコード部２４で変調され、記録／再生部２５でミニディスク１００に記録されていく、という処理が開始される。このようなコンテンツデータの受信／復号／バッファリング／エンコード／記録という処理過程において、コンテンツＩＤにかかる処理としては、サンプリングポイントＰ１のデータを監視している。そしてステップＦ３０４として、サンプリングポイントＰ１としてのサウンドユニットのデータを例えばバッファメモリ３０において確認したら、当該サウンドユニットのデータを、データストリームのバッファリングとは別に、バッファメモリ３０における他の領域に格納しておく。引き続き同様に監視を行い、ステップＦ３０５として、サンプリングポイントＰ２としてのサウンドユニットのデータを例えばバッファメモリ３０において確認したら、当該サウンドユニットのデータを、データストリームのバッファリングとは別に、バッファメモリ３０における他の領域に格納しておく。

【０２１７】ステップＦ３０６は、コンテンツデータの受信／復号／バッファリング／エンコード／記録という処理が１つのコンテンツデータに関して終了したことを示している。コンテンツデータのミニディスク１００への記録が完了したら、ステップＦ３０７で、復号処理部２８におけるＨａｓｈエンジンは、上記のようにバッファメモリ３０において格納しておいたサンプリングポイントＰ１，Ｐ２のデータを読み出し、上記式（１）（２）の演算によりコンテンツＩＤを生成する。そしてステップＦ３０８で、レコードオブジェクトレスポンスコマンドにコンテンツＩＤをセットする。このレコードオブジェクトレスポンスコマンドは、図２７のステップＦ２１１としてパーソナルコンピュータ１側に送信されることになる。

【０２１８】つまりこの処理例では、サンプリングポイントＰ１，Ｐ２のデータを、ミニディスク１００に書き込む前に抽出して格納しておくため、コンテンツＩＤ算出時にミニディスク１００を再生状態にして該サンプリングポイントのデータをシークし、読み出す必要はない。これによりコンテンツＩＤ算出処理が非常に効率化され、チェックアウトセッション時間も短縮できる。

【０２１９】次に、チェックインのためにコンテンツＩＤが要求された際に、迅速にコンテンツＩＤを送信できるようにするための処理を図３２に示す。コンテンツＩＤは、コンテンツデータ自体が記録されていることと、レングス及びトラックモードを確認できれば算出可能である。換言すれば、ミニディスク１００に記録されているコンテンツデータについては、そのコンテンツデータとＵ－ＴＯＣセクター０の情報が読み取れればサンプリングポイントＰ１，Ｐ２のデータの抽出、或いはさらにコンテンツＩＤの算出が可能である。

【０２２０】そこで図３２（ａ）の処理では、記録再生装置２０Ａに対して、ミニディスク１００が装填された際、或いはミニディスク１００が装填されている状態で電源オンとされた場合など、つまりＴＯＣデータ読出を行う時点で、サンプリングポイントＰ１，Ｐ２のデータを抽出してしまう処理を行うようにしている。

【０２２１】即ちステップＦ４０１としてＴＯＣ読出を行ったら、ステップＦ４０２で変数ｎ＝１としてステップＦ４０３に進み、まずトラック＃ｎ（＃ｎはトラックナンバ、つまり最初は第１トラック）について、サンプリングポイントＰ１，Ｐ２を算出する。Ｕ－ＴＯＣセクター０の情報が読み込まれていることで、各トラックについてのサンプリングポイントＰ１，Ｐ２の算出は可能である。そしてステップＦ４０４で、トラック＃ｎについてのサンプリングポイントＰ１，Ｐ２のデータを、実際にミニディスク１００から読出、バッファメモリ３０において特別に用意された領域に格納する。

【０２２２】ステップＦ４０５では、変数ｎが最後のトラックナンバであるか否かを判別し、最後のトラックナンバでなければステップＦ４０６で変数ｎをインクリメントしてステップＦ４０３に戻る。そしてトラック＃ｎ（即ち続いて第２トラック）についてのサンプリングポ

イントP1，P2を算出し、実際にサンプリングポイントP1，P2のデータを読み込んでバッファメモリ30に格納するという処理を行う。つまりステップF403～F406のループ処理により、ミニディスク100に収録されている全トラックについて、それぞれレングスから算出されるサンプリングポイントP1，P2のデータを読出し、バッファメモリ30に格納しておくものである。全トラックについて処理を終えたらステップF405から終了する。

【0223】一方、図28のステップF151のように、パーソナルコンピュータ1からコンテンツIDを要求された場合の処理、つまり図28のステップF252の処理は、図32（b）のようになる。即ち、ステップF451で、要求にかかるトラックナンバのトラックについてのサンプリングポイントP1，P2のデータをバッファメモリ30から読出、ステップF452で復号処理部28のHashエンジンによりコンテンツIDを算出する。なおコンテンツIDの算出のために上記式（1）（2）で必要なトラックモードやレングスは、その時点で既にバッファメモリ30に格納されているU-TOCデータから判別できる。そしてステップF453でレスポンスコマンドに生成したコンテンツIDをセットする。このレスポンスコマンドは、図28のステップF253としてパーソナルコンピュータ1に送信されることになる。

【0224】このような処理とすることで、パーソナルコンピュータ1からコンテンツIDを要求された時点において、ミニディスク100からサンプリングポイントP1，P2のデータを読み出すという必要はないため、コンテンツID要求に対応する処理を迅速化できる。全体的にみれば、チェックインセッションとしての通信時間を短縮化できる。

【0225】ところで、図32に代えて図33の処理が行われるようにしてもよい。なお、図33において図32と同一の処理は同一のステップ番号を付し説明を省略する。図33（a）の処理としては、ステップF403としてトラック#nのサンプリングポイントP1，P2を算出したら、ステップF410としてサンプリングポイントP1，P2のデータをミニディスク100から読出す。そしてそのデータは復号処理部28のHashエンジンに供給し、ステップF411としてコンテンツIDの算出を実行する。そして算出したコンテンツIDをバッファメモリ30に格納する。

【0226】このような処理をミニディスク100に収録されている全トラックに対して行う。つまり予めコンテンツIDの生成までをも行って、バッファメモリ30に格納しておくものとなる。

【0227】そしてパーソナルコンピュータ1からコンテンツIDを要求された場合の処理、つまり図28のステップF252の処理は、図33（b）のようになる。即ち、ステップF461で、要求にかかるトラックナンバのトラックについてのコンテンツIDをバッファメモリ30から読出、読み出したコンテンツIDをステップF462でレスポンスコマンドにセットする。このレスポンスコマンドは、図28のステップF253としてパーソナルコンピュータ1に送信されることになる。

【0228】このような処理とする場合、パーソナルコンピュータ1からコンテンツIDを要求された時点において、ミニディスク100からサンプリングポイントP1，P2のデータを読み出す処理や、コンテンツID算出処理は必要はないため、コンテンツID要求に対応する処理をさらに迅速化できる。

【0229】なお、図32（a）又は図33（a）の処理は、記録再生装置20Aにおいてミニディスク100からTOC読出を行う場合に実行されればよいが、例えば再生動作中或いは動作停止中など、空き時間を利用して処理を行うようにしてもよい。再生動作中としては、ミニディスクシステムでは、ディスクからのデータ読出は高速レートで間欠的に行うものであるため、間欠的な読出中断時間に、サンプリングポイントP1，P2のデータの読出を実行するようにすればよい。いずれにしても、パーソナルコンピュータ1からのコンテンツID要求に先だって図32（a）又は図33（a）の処理が行われていることで、チェックインセッションの効率化が実現できる。

【0230】13．コンテンツ書込制御フラグ

図26，図27のチェックアウトが行われた場合、ミニディスク100側では、当該チェックアウトコンテンツについては、U-TOCセクター0のトラックモードにおけるd1ビットが「1」とされることは先に述べた。このd1ビットは、ミニディスク100上に記録されたチェックアウトコンテンツについての書込制御フラグとして機能するものとなる。

【0231】d1ビットは、ミニディスクシステムにおいていわゆるライトプロテクトフラグとなる。つまりd1ビットがたてられたトラックは、消去や分割、連結などの編集が禁止される。つまり現在普及している従前のミニディスクレコーダであれ、上記記録再生装置20Aとしてのミニディスクレコーダであれ、d1ビットがたてられたトラックについては消去や分割等の編集は、行われない。ただし、実際にはミニディスクシステムにおいては、ミニディスク100上に記録されたトラックについて自動的にd1ビットがたてられることはない。従って、d1ビットは、そのトラックが編集禁止とされるだけでなく、パーソナルコンピュータ1からチェックアウトされたコンテンツであることを明示する情報となる。

【0232】本例のシステムでは、このd1ビットを書込制御フラグとして、チェックアウトコンテンツの編集を禁止するとともに、チェックイン要求の際に、そのト

ラックがチェックアウトされたものであるか否かの判別に用いるようにしている。

【0233】チェックアウトされたコンテンツデータをチェックインするには、コンテンツデータの内容が一致していることが管理上好適である。また上記のように記録再生装置20Aではコンテンツデータのレングスに基づいたサンプリングポイントP1，P2のデータを用いてコンテンツID算出を行うものであるため、もし分割或いは連結などが行われてコンテンツデータ自体のデータ長が変化してしまえば、チェックアウト時と同じコンテンツIDが生成できなくなってしまう。換言すれば、チェックアウトコンテンツが編集された場合は、コンテンツIDの不一致により適切なUsage Rule管理ができなくなり、システム処理上、チェックインを許容できないし、さらに編集により内容が変化したコンテンツデータについてチェックインを認めることは、Usage Rule管理の理念上でも適切ではない。このため、チェックアウトコンテンツについては、ミニディスク100上では編集できないようにすることが好適である。

【0234】図34に、書込制御フラグに関する記録再生装置20Aの処理を示している。なお図中「WPF」は書込制御フラグ、つまりU-TOCセクター0のトラックモードのd1ビットのことである。チェックアウトされてミニディスク100に記録されたコンテンツについては、図27のステップF212のU-TOC更新処理において、書込制御フラグWPFがオンとされる（S100）。一方、本システムにおけるチェックアウトではなく、他のソースから記録再生装置20Aもしくは他のミニディスクレコーダによってミニディスク100に記録されたコンテンツデータ（以下、自己録音コンテンツ）については、書込制御フラグWPFはオフとされたままである（S105）。

【0235】ここで、書込制御フラグWPFがオンのコンテンツデータ（トラック）については、後のチェックインを可能とするために一切の編集を禁止するという管理手法が考えられる。但し、ユーザーにチェックインができなくなることを警告した上で編集を許可するという管理手法も考えられる。

【0236】まず、チェックアウトコンテンツについての一切の編集を禁止する場合は、ユーザー操作その他により、当該コンテンツデータに対する編集指示があっても、システム制御部32は、編集禁止として、編集指示を受け付けない処理を行う（S101）。従って、チェックアウトコンテンツについては、一切編集ができないものとされ、また書込制御フラグWPFは常にオンの状態となっている（S101→S104）。

【0237】一方、自己録音コンテンツについては、もちろん自由に編集可能である（S106）。システム制御部32は、ユーザー操作その他により編集指示があれば、それに応じてMD制御部21にU-TOC更新処理を指示し、編集を実行させればよい。但し、編集が行われようと行われまいと、自己録音コンテンツに関しては常に書込制御フラグWPFはオフである（S105→S104、又はS105→S106→S104）。

【0238】チェックアウトコンテンツについて、上記のように警告を発した上で編集を許可する場合、ユーザー操作その他により編集指示があった場合は、システム制御部32はまず図7には示していない表示機能により警告としてのメッセージ出力を行う（S102）。つまり、編集することでチェックインができなくなることを警告する。これに応じてユーザーが編集指示をキャンセルした場合は、当然編集は実行されない（S102→S104）。一方、警告後さらにユーザーが編集指示を行った場合は、ユーザーがチェックイン不可となることを納得したとして編集を許可する。即ちシステム制御部32は、ユーザー操作その他の編集指示に応じてMD制御部21にU-TOC更新処理を指示し、編集を実行させる。このとき、編集にかかるトラックについての書込制御フラグWPF、つまりU-TOCセクター0の該当トラックのトラックモードのd1ビットをオフとさせる（S103）。

【0239】このような処理により、結局、チェックアウトコンテンツについては、編集が行われない限り書込制御フラグWPFはオンである。一方、編集されたチェックアウトコンテンツ、及び編集の有無に関わらず自己録音コンテンツについては、書込制御フラグWPFはオフの状態になる。従って、図28のチェックインセッションにおけるステップF151として、チェックイン対象のコンテンツIDをパーソナルコンピュータ1から要求された際、記録再生装置20AではステップF251のチェックイン可否チェックとしては、単に、当該対象とされたコンテンツデータについての、U-TOCセクター0のトラックモードの書込制御フラグWPF（d1ビット）がオンであるか否かを確認すればよいものである。

【0240】もしコンテンツIDを要求されたコンテンツデータについて書込制御フラグWPFがオフであれば、記録再生装置20Aはパーソナルコンピュータ1に対してチェックイン不可を通知すればよい。この場合は、図28のステップF253，F152としての処理によりコンテンツIDを通知/照合して、結局チェックイン不可となることという無駄な処理が解消できる。即ち、この図28のステップF253，F152の処理は、あくまで編集されていないチェックアウトコンテンツと確認されたものについて、コンテンツID照合を行う処理となり、無駄がなくなる。このためチェックイン通信セッション及び確認処理が効率化できる。

【0241】ところで、自己録音コンテンツについては編集は基本的にフリーである。しかしながら、ミニディスク100においてチェックアウトコンテンツと自己録

音コンテンツが混在しているような場合などは、自己録音コンテンツについても自由な編集を制限したい場合がある。例えばミニディスク１００におけるコンテンツデータをパーソナルコンピュータ１のアプリケーションにより管理したい場合などである。このため本例では、図２４，図２５に示したイクスクルーシブログインコントロールコマンド、イクスクルーシブログアウトコントロールコマンドが用意され、パーソナルコンピュータ１側から記録再生装置２０Ａの機能を排他制御できるようにしている。

【０２４２】パーソナルコンピュータ１から図２４のイクスクルーシブログインコントロールコマンドが記録再生装置２０Ａに送信されると、システム制御部３２は、そのプライオリティの値に応じて、編集禁止／制限のモードに入る。例えば図３４に示すように、自己録音コンテンツについても編集その他の処理の禁止又は制限が課された状態となり（Ｓ１０７）、ユーザー操作による編集指示は受け付けないものとする。なお、パワーオンやディスクイジェクトなどの操作も含めて、ユーザー操作についてどのレベルまで受け付けないかは、イクスクルーシブログインコントロールコマンドにおけるプライオリティの値による、上述した制御レベルに応じて設定されるものとなる。

【０２４３】また、イクスクルーシブログアウトコントロールコマンドが送信された場合は、それまでの編集禁止／制限は解除され、自己録音コンテンツについては編集可能となる（Ｓ１０７→Ｓ１０６）。

【０２４４】このようなイクスクルーシブログインコントロールコマンドにより、パーソナルコンピュータ１側が記録再生装置２０Ａ側の機能を排他制御できることで、システム動作の都合に応じて、編集等を制限できるため、システム動作上、便利なものとなる。

【０２４５】１４．課金情報処理

続いて、課金情報処理について説明する。図３６はコンテンツデータ配信に対する課金処理のためのシステム構成を示している。なお、このシステム構成は図４と同様であるが、コンテンツサーバ９１側の構成を詳しく示したものである。

【０２４６】上述してきたように本例のシステムは、コンテンツとしての楽曲データ等をサーバ９１側から一次記録媒体（ＨＤＤ５）にダウンロードし、さらに二次記録媒体（ミニディスク１００）にチェックアウトできるシステムである。もちろんコンテンツサーバ９１が、コンテンツデータを有料で提供することが考えられる。

【０２４７】この場合コンテンツサーバ９１は、コンテンツ提供サービスを行う組織や個人によって運営されるもので、基本的には、各種コンテンツを蓄積するコンテンツ保有機能、ネットワーク１１０を介した通信によりパーソナルコンピュータ１に対して保有しているコンテンツを提供する機能、コンテンツ提供を受けるユーザーに対する課金管理を行う課金機能、を有するものとなる。これらの各機能は、１つの組織、会社等によって全体的に運営されてもよいが、それぞれが異なる組織、会社、個人等によって運営され、連係的に動作されるものであってもよい。例えば各機能のそれぞれがインターネット上のウエブサイトとして運営され、互いにリンクにより連係動作がとられるようにしてもよい。

【０２４８】ユーザーサイドで最終的にコンテンツデータが記録される二次記録媒体としては、ミニディスク１００やメモリカードとして述べてきたが、この二次記録媒体としてのメディアには、後述するプリベイド情報が書換不能に記録されている。コンテンツサーバ９１側は、二次記録媒体に記録されているプリベイド情報を受け取ることで、個々のユーザに対する課金処理を行うものとなる。

【０２４９】コンテンツサーバ９１は、ネットワーク配信装置１３０、コンテンツデータベース制御装置１４０、顧客情報装置１５０、コンテンツデータベース１６０、顧客データベース１７０を有して構成される。ネットワーク配信装置１３０は、ネットワーク１１０を介してパーソナルコンピュータ１等に、保有しているコンテンツを提供する機能を実現する部位である。コンテンツデータベース制御装置１４０及びコンテンツデータベース１６０は、各種コンテンツを蓄積するコンテンツ保有機能を実現する部位である。顧客情報装置１５０及び顧客データベース１７０は、コンテンツ提供を受けるユーザに対する課金管理を行う課金機能を実現する部位である。

【０２５０】コンテンツデータベース１６０は例えばハードディスク、光ディスクなどの記録媒体により形成され、このコンテンツデータベース１６０には、例えば多数の音楽コンテンツが、ユーザーに対する提供サービス用のコンテンツとして音楽ライブラリ形式で格納されている。コンテンツデータベース制御装置１４０は、コンテンツデータベース１６０に対して音楽コンテンツ等の記録、読出を制御する。例えばネットワーク配信装置１３０からの要求に応じてコンテンツデータベース１６０からコンテンツを読出、ネットワーク配信装置１３０に提供する。

【０２５１】顧客データベース１７０は、例えばハードディスク、光ディスクなどの記録媒体により形成され、この顧客データベース１７０には、個々の二次記録媒体１００に記録されているプリベイド情報に対応して、課金情報が登録されている。顧客情報装置１５０は、顧客データベース１７０に対して課金情報の登録や読出の制御を行う。例えばネットワーク配信装置１３０からの要求に応じて、新規に課金情報を顧客データベース１７０に登録したり、或いは特定の課金情報を読み出してネットワーク配信装置１３０に提供する。

【０２５２】これらコンテンツサーバ９１としての各部

位は、上述したように１つの組織、会社、個人等により運営されてもよいし、それぞれ異なる組織等によって運営されてもよい。例えばネットワーク配信装置１３０は配信サービス会社によって運営され、コンテンツデータベース制御装置１４０及びコンテンツデータベース１６０はレコード会社、レコードレーベル会社等によって運営され、顧客情報装置１５０及び顧客データベース１７０は課金サービス会社によって運営されるという形態もあり得る。また、例えばコンテンツデータベース制御装置１４０及びコンテンツデータベース１６０は複数存在し、ネットワーク配信装置１３０がそれぞれのコンテンツデータベース１６０に格納されているコンテンツを配信できるような形態もあり得る。

【０２５３】このような本例のシステムでは、パーソナルコンピュータ１はコンテンツサーバ９１との間で通信接続を行い、提供可能なコンテンツのリスト（メニュー）を受け取る。ユーザーはリストの中で所望のコンテンツを選択する操作を行う。するとコンテンツサーバ９１側からそのコンテンツがパーソナルコンピュータ１に送信されてくる。ユーザーサイドではそのコンテンツを上述してきたチェックアウトにより二次記録媒体１００に記録する。これによってユーザーは所望の楽曲等を入手できるものとなる。そして本例では、コンテンツの対価の課金に関しては、二次記録媒体１００に記録されているプリペイド情報を利用する。後述するが、二次記録媒体１００にはプリペイド情報として個々のメディア毎に異なるメディアＩＤとプリペイド金額が含まれている。パーソナルコンピュータ１は記録再生装置２０Ａ（２０Ｂ）からプリペイド情報を受け取って、そのプリペイド情報をコンテンツサーバ９１側に送信する。ネットワーク配信装置１３０はそのプリペイド情報に基づいて顧客データベース１７０上で課金処理を実行させる。大まかにいえば、顧客データベース１７０には各二次記録媒体１００のプリペイド情報に対応して課金情報が登録されており、コンテンツ配信に応じてその対価額を課金情報におけるプリペイド金額から減算していく。つまり課金は顧客データベース１７０上での課金情報の更新により行われる。そして二次記録媒体１００側に記録されているプリペイド情報については、一切書換は行われないものである。

【０２５４】顧客データベース１７０には、図３７のような課金情報が登録される。ここでいう課金情報とは、１つのプリペイド情報（１つの二次記録媒体１００）に対応して登録されるデータ群をいい、例えばメディアＩＤ、残り金額、購入履歴などのデータから１つの課金情報が構成される。図３７にはメディアＩＤとしてのＩＤ１～ＩＤ５・・・のそれぞれに対応して課金情報Ｋ１～Ｋ５・・・が登録されている様子を例示している。

【０２５５】課金情報におけるメディアＩＤとは、後述するプリペイド情報に含まれているメディアＩＤである。残り金額とは、プリペイド元金からコンテンツ購入毎にその代金が引かれていくように更新されることで、現在でのプリペイド残金を示す情報である。購入履歴とは、購入日時、コンテンツ名、コンテンツ金額、使用端末などの履歴であり、つまりコンテンツ購入毎にその状況を記録した情報となる。なお、もちろんこれら以外の情報としてプリペイド元金や、メディア種別、メディア販売者、購入コンテンツの著作権者などの多様な情報が課金情報に含まれてもよいし、また例えば購入履歴は含まれなくてもよい。本例の配信動作に関していえば、少なくともメディアＩＤと残り金額の情報が課金情報として含まれていればよく、他の情報は配信システムの運営上の都合やサービス内容などに応じて設定すればよい。

【０２５６】プリペイド情報は、二次記録媒体１００において書換不能に記録されている情報であり、基本的に図３８に示すようにプリペイド金額、プリペイドサービスＩＤ、メディアＩＤから構成される。プリペイド金額とは、ユーザーが先払いとして支払った金額が記録される。二次記録媒体１００は、例えばコンテンツとしては何も記録されていない未使用のミニディスクやメモリカードとして販売されるが、その販売価格はプリペイド金額を含むものとされる。つまり、未使用の場合の通常の販売価格が５００円のメディアであるとしたときに、プリペイド情報においてプリペイド金額が５０００円と記録されている二次記録媒体１００の場合は、基本的には５５００円でユーザーが購入するものとなる。もちろん販売価格は任意であり、上記二次記録媒体１００が、メディア自体は無料とされてプリペイド金額のみの５０００円で販売されたり、或いは４８００円にディスカウントされて販売されてもかまわないが、プリペイド金額が５０００円と記録された二次記録媒体１００を購入したユーザーは、本例の配信システムによるコンテンツ配信サービスに関して、５０００円を先払いしたこととなる。

【０２５７】プリペイドサービスＩＤは、コンテンツ配信サービスを行うコンテンツサーバ９１のアドレスを表す。例えばネットワーク１１０においてネットワーク配信装置１３０に通信接続するためのアドレスである。インターネットにおけるＩＰアドレスであってもよい。パーソナルコンピュータ１は、記録再生装置２０Ａに装填された二次記録媒体１００についてのプリペイド情報を受け取ることで、プリペイドサービスＩＤに基づいて、コンテンツサーバ９１に通信アクセスを行い、接続を求めることができる。なおコンテンツサーバ９１側の構成にもよるが、プリペイドサービスＩＤは、ネットワーク配信装置１３０のアドレスではなく、例えばコンテンツデータベース制御装置１４０のアドレスとしたり、或いは顧客情報装置１５０のアドレスとしてもよい。例えばネットワーク配信装置１３０、コンテンツデータベース制御装置１４０、顧客情報装置１５０がそれぞれインタ

ーネット上のＷｅｂページとして形成され、互いにリンクされるような場合、プリペイドサービスＩＤをコンテンツデータベース制御装置１４０のアドレスとして、パーソナルコンピュータ１はコンテンツデータベース制御装置１４０に対して通信アクセスを行うようにし、その際に、配信処理の進行に応じて顧客情報装置１５０がリンクされ、さらにこれらがネットワーク配信装置１３０によって統括処理されるようにすることも考えられる。逆にプリペイドサービスＩＤを顧客情報装置１５０のアドレスとして、パーソナルコンピュータ１は顧客情報装置１５０に対して通信アクセスを行うようにし、その際に、配信処理の進行に応じてコンテンツデータベース制御装置１４０がリンクされ、さらにこれらがネットワーク配信装置１３０によって統括処理されるようにすることも考えられる。

【０２５８】メディアＩＤは、個々の二次記録媒体１００についてそれぞれ固有に付された識別ナンバである。例えばユーザーが２枚のプリペイドメディアとしての二次記録媒体１００を購入した場合、その各二次記録媒体１００には、それぞれ異なるメディアＩＤが記録されていることになる。

【０２５９】このようなプリペイド情報は、例えばプリペイド金額に８ビット、プリペイドサービスＩＤに２２ビット～３２ビット程度、メディアＩＤに３２～４０ビット程度を用いたデータとすることができる。ビット数はプリペイドシステムの設計上の都合で決められればよい。またプリペイドサービスＩＤには、サーバのアドレス等のために必要なビット数、メディアＩＤには、販売するプリペイドメディアの総数や将来的な総数などを勘案して、個々に異なるＩＤナンバを降ることができるために十分なビット数とされればよい。最低限としては、例えばプリペイド金額に１バイト（８ビット）、プリペイドサービスＩＤに３バイト又は４バイト、メディアＩＤに３バイト又は４バイトとして、８バイト程度のデータとされればよい。

【０２６０】ここで、二次記録媒体１００に記録されるプリペイド情報と、図３７に示した課金情報の関係について述べておく。例えばメディアＩＤ＝ＩＤ１、プリペイド金額＝５０００円とされた二次記録媒体１００をユーザーが使用したとする。コンテンツサーバ９１側では、この二次記録媒体１００が最初に使用された時点で、顧客データベース１７０に、図３７の課金情報Ｋ１を登録する。当初、この課金情報Ｋ１におけるメディアＩＤ及び残り金額は、プリペイド情報上のデータがそのまま登録されることになり、つまり課金情報Ｋ１のメディアＩＤ＝ＩＤ１とされ、残り金額＝５０００円とされる。その後、その二次記録媒体１００を使用してコンテンツのダウンロード（二次記録媒体１００へのチェックアウト）が行われることに応じて、そのコンテンツの代価が、課金情報Ｋ１の残り金額の減額という形で課金処理されることになる。つまり、ダウンロード／チェックアウトが行われる毎に、使用されている二次記録媒体１００のプリペイド情報におけるメディアＩＤから、顧客データベース１７０上で対応する課金情報が検索され、その課金情報上で残り金額の減算が行われる。例えば図３７の課金情報Ｋ１では残り金額が３７００円とされているが、これはユーザーがメディアＩＤ＝ＩＤ１の二次記録媒体１００を用いて、１３００円分のコンテンツ購入を行った後の状態として示されているものとなる。

【０２６１】そしてこのような課金処理方式からわかるように、ユーザーが所有する二次記録媒体１００においてはプリペイド情報は全く更新されないものとなり、換言すれば、プリペイド情報は二次記録媒体１００において書換不能に記録されていればよいものとなる。なお、プリペイド情報は二次記録媒体１００において書換可能としてもよいが、プリペイド金額やメディアＩＤの改竄による悪用や、プリペイドサービスＩＤの改竄によるサービス動作の不具合のおそれもあるため、書換不能とすることが適切である。

【０２６２】上述のように二次記録媒体１００としてミニディスクを使用する場合において、８バイトのプリペイド情報を書換不能に記録しておく記録方式は次のような各例が考えられる。

（１）Ｐ－ＴＯＣ内にプリペイド情報を記録する

（２）Ｕ－ＴＯＣ内に書換不能となる手法でプリペイド情報を記録する。

（３）管理エリア内でＵ－ＴＯＣ領域外に書換不能となる手法でプリペイド情報を記録する。

【０２６３】Ｐ－ＴＯＣ内にプリペイド情報を記録する場合は、例えば図９（ａ）のリードインエリアにおけるＰ－ＴＯＣセクターにおいて特定の８バイトの領域を、プリペイド情報の記録に用いることが考えられる。

【０２６４】Ｕ－ＴＯＣ内に記録する場合は、例えば既にフォーマットが規定されているセクター０，１，２，３，４などにおける未使用の領域を利用してもよいが、プリペイド情報が書換えられる可能性を適切に排除するには、まだ規定されていないセクターを利用することが考えられる。例えばＵ－ＴＯＣセクター５において所定の８バイトをプリペイド情報の記録領域として設定するものである。そしてさらにこの場合は、上述したＵ－ＴＯＣセクター０において、セクター使用状況（Used sectors）におけるセクター５の対応ビットを「０」、つまり使用していないセクターとして表されるようにすることで、プリペイド情報を書換不能とできる。つまりこれにより一般のミニディスクレコーダによれば、Ｕ－ＴＯＣセクター５は使用されていないセクターとして認識されるため、Ｕ－ＴＯＣセクター５について何らかの更新処理等が行われることはない。つまりプリペイド情報はユーザーサイドで書換不能とされる。そして本例の記録再生装置２０Ａでは、プリペイド情報の読出のためのアプ

リケーションプログラムに基づいて、U－TOCセクター5の読込を実行するものとされていることにより、プリペイド情報を読み出すことができる。なお、ここではセクター5としたが、もちろんセクター6、セクター7など他のセクターを利用してもよい。

【0265】また図9（b）の管理エリア内であって、U－TOC以外の領域に記録する方式として、例えば斜線部PDとして示すように、使用されていないクラスタ内のセクターを利用してプリペイド情報を記録することが考えられる。管理エリア内ではパワーキャリブレーションエリアPCAやU－TOCエリアが形成され、これらの位置は上述したようにP－TOCによって示されるものとなる。P－TOCを参照することによって通常のミニディスクレコーダはパワーキャリブレーションエリアPCAやU－TOCエリアにアクセスできる。ところがP－TOCによって位置が示されていない斜線部PDは、通常のミニディスクレコーダではアクセスできない領域（アクセスしても意味のない領域）となる。従って、斜線部PDに記録されたプリペイド情報はユーザーサイドで書換不能とされる。そして本例の配信システムに用いる記録再生装置20Aでは、プリペイド情報の読出のためのアプリケーションプログラムに基づいて、斜線部PDの読込を実行するものとされていることにより、プリペイド情報を読み出すことができる。このためには例えば、斜線部PDの開始位置を、P－TOCに示されるU－TOCスタートアドレスに所定量のオフセットを与えた位置と規定しておくことで、記録装置10によってプリペイド情報の読出が可能となる。例えばU－TOCは3クラスタにわたって記録されるため、U－TOCスタートアドレスUSTA＋5クラスタの位置をプリペイド情報記録領域の開始位置と規定すればよい。

【0266】例えば以上の例のようにすることで、ミニディスクをプリペイドメディア4として用いることができる。またミニディスクについて説明したが、二次記録媒体100としてメモリカードや、CD－R、CD－RW、DVD等の光ディスクの場合についても、8バイト或いはそれ以上のデータサイズのプリペイド情報を記録する場合は、それらのメディアの管理フォーマット等に基づいて、記録位置が設定されればよい。

【0267】ところで、このようなプリペイド情報を用いた配信システムを構築する場合、パーソナルコンピュータ1は記録再生装置20Aに装填された二次記録媒体（ミニディスク100）についてのプリペイド情報を読み出せるようにする必要がある。このため、図20，図21で説明したようにチェックインコントロールコマンドにおいてサブファンクションでプリペイド情報を指定することで、記録再生装置20Aにプリペイド情報を要求できるようにしている。また記録再生装置20Aは、図23のチェックインレスポンスコマンドによって、ミニディスク100に記録されているプリペイド情報をパーソナルコンピュータ1に通知できる。

【0268】図35は、プリペイド情報処理のための処理を示している。図35において、パーソナルコンピュータ1のCPU2が実行する制御処理をステップF101～F173とし、また記録再生装置20Aのシステム制御部32、MD制御部21等によって実行される制御処理をステップF201～F274として示している。通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【0269】この場合も、認証開始からEKB転送、ルートキー探索等の処理は上記チェックアウトの場合と同様に行われる。即ち上記図26、図28と同一のステップ番号を付したステップF101～F103、F201～F205は、上述と同様の処理が行われるものであり、重複説明を避ける。

【0270】パーソナルコンピュータ1はステップF170で、セッションの開始を要求するコントロールコマンドを送信する。これに応じて記録再生装置20Aはステップ270で、レスポンスコマンドを返す。なお、この場合にも、図12で説明した認証処理が行われる。

【0271】セッションが開始され、且つ記録再生装置20Aが認証OKとなったら、パーソナルコンピュータ1はステップF171として、プリペイド情報を要求する。つまり、図20で説明したチェックインコントロールコマンドを送信するものとなる。このときチェックインコントロールコマンドにおいては、サブファンクションの値は「00h」又は「01h」ではなく、つまりプリペイド情報要求の意味を持たせたものとする（図21参照）。

【0272】記録再生装置20Aは、これに応じてステップF271で、上述のようにミニディスク100の特定の領域に記録されているプリペイド情報を再生する。そしてステップF272で、再生した例えば8バイトのプリペイド情報を、図23のようにチェックインレスポンスコマンドにセットして、パーソナルコンピュータ1に送信する。

【0273】チェックインレスポンスコマンドによりプリペイド情報を受け取ったら、パーソナルコンピュータ1はステップF172でセッション終了要求のコントロールコマンドを記録再生装置20Aに送信する。記録再生装置20Aはステップ273としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ1に送信する。またパーソナルコンピュータ1はステップF173で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置20Aはステップ274で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、プリペイド情報受け渡しのための通信が終了される。

【0274】その後、パーソナルコンピュータ1はプリペイド情報に対する処理として、通信部8によりネット

ワーク１１０を介してコンテンツサーバ９１と通信接続し、受け取ったプリペイド情報を、コンテンツサーバ９１に転送する処理を行う。即ち、二次記録媒体１００に対してチェックアウトしたコンテンツデータの識別情報とともにプリペイド情報を送信することで、コンテンツサーバ９１側でユーザーに対する課金処理、即ち図３７のデータベースの更新処理が行われるようにするものである。

【０２７５】このようにパーソナルコンピュータ１が記録再生装置２０Ａに対して二次記録媒体１００における固有情報であるプリペイド情報の転送を要求できることで、当該システムによるプリペイド方式の課金処理が可能となる。

【０２７６】なお、本例としてパーソナルコンピュータ１が二次記録媒体１００の固有情報としてプリペイド情報を取得する方式を述べたが、同様のコントロールコマンド及びレスポンスコマンドの設定によって、各種の固有情報取得が可能となることはいうまでもない。例えば二次記録媒体１００に記録されたユーザーの利用状況、ユーザーＩＤなど、他の固有情報をパーソナルコンピュータ１が取得することで、パーソナルコンピュータ１が二次記録媒体１００の管理を行ったり、或いはそれらの情報をコンテンツサーバ９１に送信して、コンテンツサーバ９１側がユーザーに対する各種サービスや管理に用いることが想定できる。

【０２７７】以上、実施の形態としての例を説明してきたが、本発明は上記例に限定されるものではない。システム動作としての暗号化、データパス、チェックアウト／チェックイン方式、認証方式、コンテンツＩＤ生成方式、コンテンツＩＤ管理方式、書込制御フラグの実際の例、編集管理、プリペイド情報などは、それぞれ発明の要旨の範囲内で各種変形例が考えられる。

【０２７８】また本発明としては、例えば上述してきた一次記録媒体から二次記録媒体へのデータ転送処理の対象となるのはＳＤＭＩコンテンツに限られず、各種のコンテンツデータに広く適用できる。また一次記録媒体はＨＤＤ以外に多様に考えられる。もちろん二次記録媒体、二次記録媒体側機器２０Ａとしてもミニディスク、ミニディスク記録装置に限らず、多様な例が考えられる。二次記録媒体１００としては、ＣＤ−Ｒ、ＣＤ−ＲＷ、ＤＶＤ−ＲＡＭ、ＤＶＤ−Ｒ、ＤＶＤ−ＲＷ、各種メモリカードなどであってもよい。従って二次記録媒体側機器２０Ａは、これらのメディアに対応する記録装置であればよい。また、ＳＤＭＩ対応の記録再生装置２０Ｂについても言及したが、その記録再生装置２０Ｂへのコンテンツデータの転送処理においても本発明は適用できる。

【０２７９】

【発明の効果】以上の説明からわかるように本発明によれば、データ転送装置側（一次記録媒体側）では、格納されている各コンテンツデータについての転送権利を管理するとともに、データ記録装置（二次記録媒体側）に対して転送したコンテンツデータについては、そのコンテンツデータに対応する第１のコンテンツ識別子とデータ記録装置側から送信されてきた第２のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理するようにしている。つまり、二次記録媒体側でコンテンツ識別子（コンテンツＩＤ）を記録できない場合でも、二次記録媒体側で発生させるコンテンツＩＤ（第２のコンテンツ識別子）を用いて二次記録媒体上のコンテンツデータを識別でき、しかもそれが一次記録媒体側のコンテンツＩＤ（第１のコンテンツ識別子）と対応づけられているため、コンテンツＩＤによる適切なチェックアウト／チェックイン時の権利管理が可能となる。従って非ＳＤＭＩ対応の二次記録媒体においてコンテンツデータを非暗号化状態で記録する場合にも、コピー転送や再生に関してのコンテンツ権利が適切に管理でき、ユーザーの利便性と著作権保護を両立できる。

【０２８０】また、二次記録媒体に対する記録再生を行うデータ記録装置側での第２のコンテンツ識別子の生成に関しては、非暗号化状態のコンテンツデータの一部を抽出した演算で第２のコンテンツ識別子を生成することで、各コンテンツデータ毎に固有のコンテンツＩＤとして生成できる。また、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツＩＤ生成に用いるコンテンツデータの一部を抽出するというように、抽出ポイントが設定されていることで、各コンテンツデータについては、常にそれぞれ特定のコンテンツＩＤを生成できる。つまり第２のコンテンツ識別子自体を記録しておかなくても、二次記録媒体側のコンテンツデータから特定の第２のコンテンツ識別子を常に得られるため、上記の権利管理に用いる情報として好適なものとなる。また、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた１又は複数のポイントとすることで第２のコンテンツ識別子を、各コンテンツデータに固有の情報として適切なものとできる。例えばオーディオコンテンツの場合、先頭及び終端は無音状態などであって、データ自体が他のコンテンツと同じものとなっている場合が多いが、それ以外の部分は、データ自体が他のコンテンツと同じということはまずあり得ないからである。

【０２８１】また、チェックアウトとしてデータ転送装置からコンテンツデータが転送されてくる際には、復号されたコンテンツデータを二次記録媒体に記録するまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により第２のコンテンツ識別子を生成するようにすることで、第２のコンテンツ識別子の算出のために、二次記録媒体に読出アクセスを行ってサンプリングポイントのデ

ータを得るという動作は不要となる。従ってチェックアウト時に、データ転送装置側に第2のコンテンツ識別子を通知する処理を効率化でき、一連のチェックアウト通信動作を高速化できる。

【0282】また、コンテンツデータが記録された二次記録媒体がデータ記録装置に装填されている場合には、チェックイン要求が無い時点で、二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶させておくこと、或いは更に第2のコンテンツ識別子の算出までを行って記憶させておくことで、チェックイン等のために第2のコンテンツ識別子が要求された際に、二次記録媒体のアクセスは不要である。従ってこの場合もチェックイン等のための一連の通信動作を高速化できる。

【図面の簡単な説明】

【図1】本発明の実施の形態で利用される暗号化方式のツリー構造の説明図である。

【図2】実施の形態で利用される暗号化方式のEKBの説明図である。

【図3】実施の形態で利用される暗号化方式のEKBの構造の説明図である。

【図4】実施の形態のシステム構成のブロック図である。

【図5】実施の形態のSDMIコンテンツのデータバス例の説明図である。

【図6】実施の形態の一次記録媒体側機器のブロック図である。

【図7】実施の形態の二次記録媒体側機器のブロック図である。

【図8】ミニディスクシステムのクラスタフォーマットの説明図である。

【図9】ミニディスクのエリア構造の説明図である。

【図10】ミニディスクシステムのU-TOCセクター0の説明図である。

【図11】ミニディスクシステムのU-TOCセクター0のリンク形態の説明図である。

【図12】実施の形態の認証処理のフローチャートである。

【図13】実施の形態の配信／転送されるコンテンツデータ及び暗号化状態の説明図である。

【図14】実施の形態の暗号化方式例及びDNKの説明図である。

【図15】実施の形態のコンテンツデータの暗号解除手順の説明図である。

【図16】実施の形態のチェックアウトコントロールコマンドの説明図である。

【図17】実施の形態のチェックアウトレスポンスコマンドの説明図である。

【図18】実施の形態のレコードオブジェクトコントロールコマンドの説明図である。

【図19】実施の形態のレコードオブジェクトレスポンスコマンドの説明図である。

【図20】実施の形態のチェックインコントロールコマンドの説明図である。

【図21】実施の形態のチェックインコントロールコマンドのサブファンクションの説明図である。

【図22】実施の形態のチェックインレスポンスコマンドの説明図である。

【図23】実施の形態のチェックインレスポンスコマンドの説明図である。

【図24】実施の形態のイクスクルーシブログインコントロールコマンドの説明図である。

【図25】実施の形態のイクスクルーシブログアウトコントロールコマンドの説明図である。

【図26】実施の形態のチェックアウト動作のフローチャートである。

【図27】実施の形態のチェックアウト動作のフローチャートである。

【図28】実施の形態のチェックイン動作のフローチャートである。

【図29】実施の形態のコンテンツID生成の説明図である。

【図30】実施の形態のコンテンツID対応テーブルの説明図である。

【図31】実施の形態のチェックアウト時のコンテンツID生成処理のフローチャートである。

【図32】実施の形態のチェックイン前のコンテンツID生成処理のフローチャートである。

【図33】実施の形態のチェックイン前のコンテンツID生成処理のフローチャートである。

【図34】実施の形態の書込制御フラグによる動作の説明図である。

【図35】実施の形態の課金情報読出動作のフローチャートである。

【図36】実施の形態の課金管理システムの説明図である。

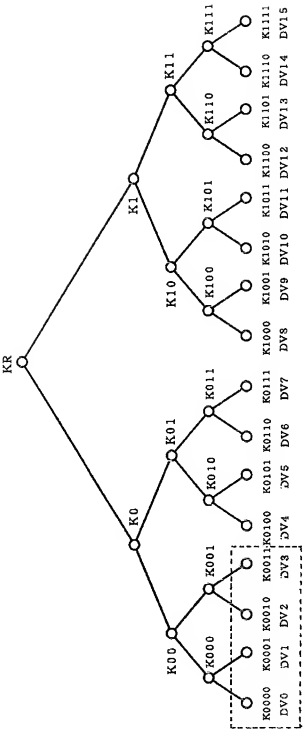
【図37】実施の形態の顧客データベースの説明図である。

【図38】実施の形態のプリペイド情報の説明図である。

【符号の説明】

1　一次記録媒体側機器（パーソナルコンピュータ）、2　CPU、5　HDD（一次記録媒体）、8　通信部、9　ディスクドライブ、11　接続部、20A　二次記録媒体側機器（記録再生装置）、21　MD制御部（CPU）、25記録／再生部、26　インターフェース部、28　復号部、30　バッファメモリ、31　システム制御部、100　二次記録媒体（ミニディスク）

【図1】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000 K0001 K0010 K0011 K0100 K0101 K0110 K0111 K1000 K1001 K1010 K1011 K1100 K1101 K1110 K1111
DV0 DV1 DV2 DV3 DV4 DV5 DV6 DV7 DV8 DV9 DV10 DV11 DV12 DV13 DV14 DV15
デバイス

【図2】

(a)

有効化キーブロック(EKB:Enabling Key Block) 例1

デバイスDV0, DV1, DV2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	E(K(t)0,K(t)R)
00	E(K(t)00,K(t)0)
000	E(K000,K(t)00)
001	E(K(t)001,K(t)00)
0010	E(K0010,K(t)001)

(b)

有効化キーブロック(EKB:Enabling Key Block) 例2

デバイスDV0, DV1, DV2にバージョン:tのノードキーを送付

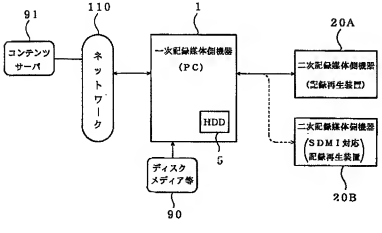
バージョン(Version):t	
インデックス	暗号化キー
000	E(K000,K(t)00)
001	E(K(t)001,K(t)00)
0010	E(K0010,K(t)001)

【図3】

EKB(Enabling Key Block)の構造例

オフセットアドレス	内容	サイズ(byte)
0	ノードキーの数	4
4	ノードキーの深さ	4
8	EKBバージョン	4
12	リザーブ	4
16	暗号化された各ノードキー	16×M
16+16×M	リザーブ	16
32+16×M	暗号化EKBバージョン	8
40+16×M	電子署名	5

【図4】



【図16】

Check Out Control Command

オフセット(バイト)	MSB 7 6 5 4 3 2 1 0 LSB	
00h	CTS	o type : CONTROL
⋮	⋮	
0Ah	Op Code : Check Out	
0Bh	result	
0Ch	Reserved	
0Dh	List ID	
0Eh		
0Fh	object position number	
10h		
11h ⋮ 18h	DES CBC (ks,0)	

【図17】

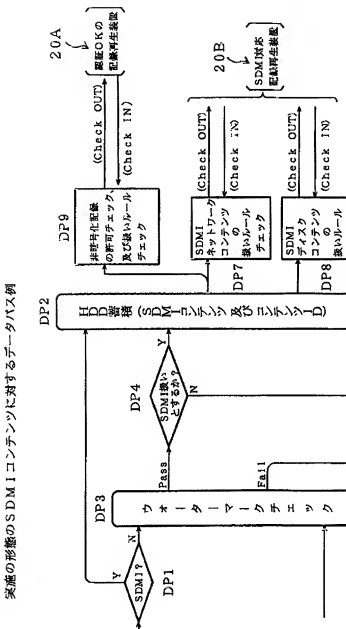
Check Out Response Command

オフセット(バイト)	MSB 7 6 5 4 3 2 1 0 LSB	
00h	CTS	response : ADDEPTI D
⋮	⋮	
0Ah	Op Code : Check Out	
0Bh	result	
0Ch	Reserved	
0Dh	List ID	
0Eh		
0Fh	object position number	
10h		

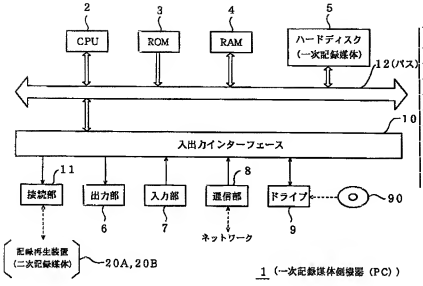
【図21】

値	Subfunction
00h	コンテンツ ID
01h	reserved
他	プリペイド情報

【図5】


実施の形態のSDMIコンテンツに対するデータパス例
ネットワークコンテンツ
(SDMI準拠コンテンツ又は非SDMIコンテンツ)
ディスクコンテンツ
SDMI?
Y
N
DP1
DP2
HD装置(SDMIコンテンツ及びノンSDMIコンテンツ)
DP3
ウォーターマークチェック
Pass
Fail
SDMI扱いとするか?
DP4
非SDMI扱い
ピー不可扱い
DP5
DP6
DP7
DP8
DP9
非許可化装置の許可チェック、及び扱いルールチェック
(Check OUT)
(Check IN)
SDMIネットコンテンツの扱いルールチェック
SDMIディスクコンテンツの扱いルールチェック
20A
20B
装置のOKの記録再生装置
SDMI技術記録再生装置

【図6】

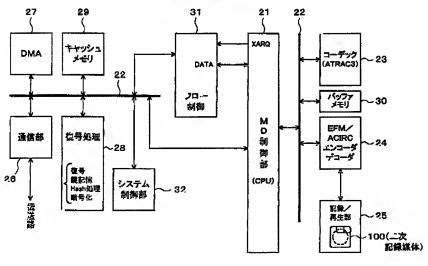


【図20】

Check In Control Command

オフセット(バイト)	MSB 7	6	5	4	3	2	1	LSB 0
00h	CTS				c type : CONTHOL			
⋮	⋮							
0Ah	Op Code : Check In							
0Bh	result							
0Ch	Subfunction							
0Dh	List ID							
0Eh								
0Fh	object position number							
10h								

【図7】



【図24】

Exclusive Login Control Command

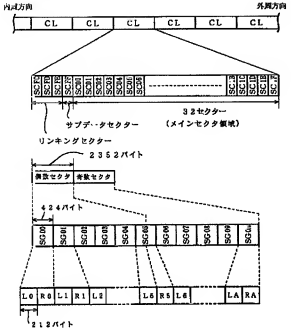
オフセット(バイト)	MSB 7	6	5	4	3	2	1	LSB 0
00h	CTS				c type : CONTHOL			
01h	subunit type				subunit ID			
02h	Reserved							
03h	priority							

【図25】

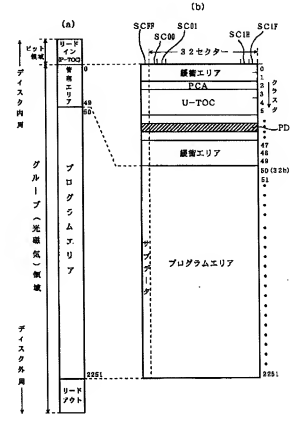
Exclusive Logout Control Command

オフセット(バイト)	MSB 7	6	5	4	3	2	1	LSB 0
00h	CTS				c type : CONTROL			
01h	subunit type				subunit ID			
02h	Reserved							
03h	priority : 00h							

【図8】

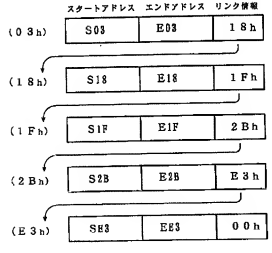


【図9】

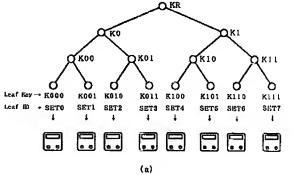


【図11】

P−FRA= 03h



【図14】

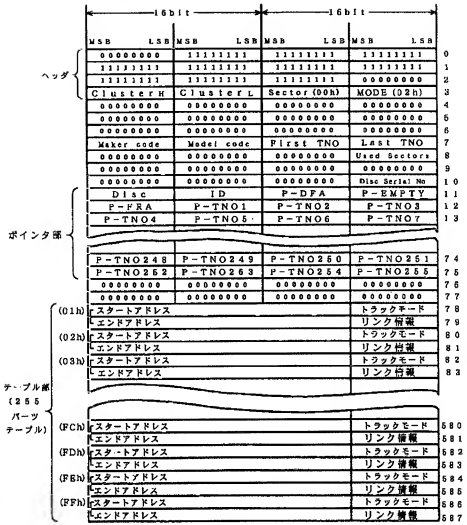


SET0のDNK (Device Node Key) 例

Leaf ID=SET0
Leaf Keyで暗号化したKR E(K000,KR)
Leaf Keyで暗号化したK0 E(K000,K0)
Leaf Keyで暗号化したK00 E(K000,K00)
Leaf Key=K000

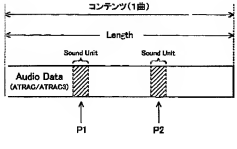
(b)

【図10】

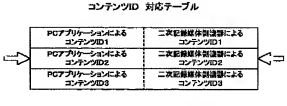


U-TOCセクター0

【図29】

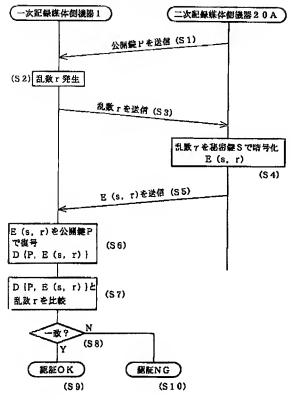


【図30】



【図12】

認証処理例



【図15】

EKB

E (K0, KR')

コンテンツキー

E (KR', CK)

コンテンツデータ

E (CK, A3D)

SET0のDNK

Leaf ID=SET0
Leaf Key=K000
E (K000, KR)
E (K000, K0)
E (K000, K00)

①リーフキー「K000」からノードキー「K0」を解読
D {K000, E (K000, K0)} =K0

②ノードキー「K0」からルートキー「KR」を解読
D {K0, E (K0, KR')} =KR'

③ルートキー「KR」からコンテンツキー「CK」を解読
D {KR', E (KR', CK)} =CK

④コンテンツキー「CK」からコンテンツデータ「A3D」を解読
D {CK, E (CK, A3D)} =A3D

【図18】

Record Object Control Command

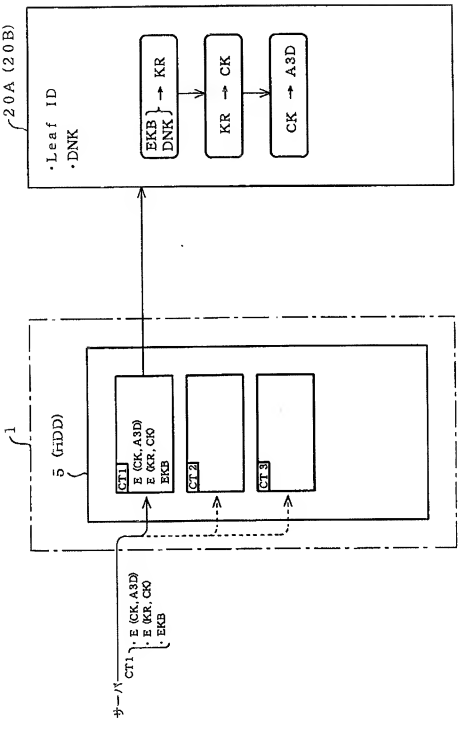
オフセット (バイト)	MSB 7 6 5 4 3 2 1 0 LSB
00h	CTS / c type : CONTROL
⋮	⋮
0Ah	Op Code : Record Object
0Bh	result
0Ch	Reserved
0Dh	
0Eh	
0Fh	Destination List ID
10h	
11h	new object position number
12h	
13h	content type
14h	Download Format Track Attribute
15h	Track Mode
16h	Content Size
17h	
18h	
19h	
1Ah	Bulk Data Size
1Bh	
1Ch	
1Dh	

【図19】

Record Object Response Command (Accepted)

オフセット (バイト)	MSB 7 6 5 4 3 2 1 0 LSB
00h	CTS / response : ACCEPTED
⋮	⋮
0Ah	Op Code : Record Object
0Bh	result
0Ch	Reserved
0Dh	
0Eh	
0Fh	Destination List ID
10h	
11h	new object position number
12h	
13h	content type
14h	Download Format Track Attribute
15h	Track Mode
16h	Content Size
17h	
18h	
19h	
1Ah	Bulk Data Size
1Bh	
1Ch	
1Dh	
1Eh ⋮ 3Dh	Session DATA (32 byte) (コンテンツ ID)

【図13】


20A (20B)
・Leaf ID
・DNK
EKB
DNK
KR
KR
CK
CK
A3D
1
5 (HDD)
CT1
E (CK, A3D)
E (KR, CK)
EKB
CT2
CT3
サーバ
CT1
E (CK, A3D)
E (KR, CK)
EKB

【図22】

Check In :Response Command

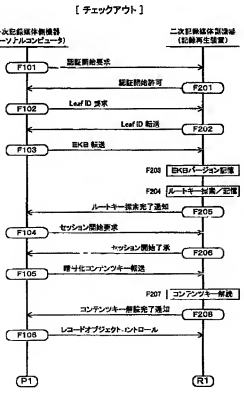
オフセット (バイト)	MSB 7	6	5	4	3	2	1	LSB 0
00h	CTS				response : ACCEPTED			
⋮	⋮							
0Ah	Op Code : Check In							
0Bh	result							
0Ch	Subfunction							
0Dh	List ID							
0Eh								
0Fh	object position number							
10h	Hash MAC (コンテンツ ID)							
11h								
12h								
13h								
14h								
15h								
16h								
17h								
18h								

【図23】

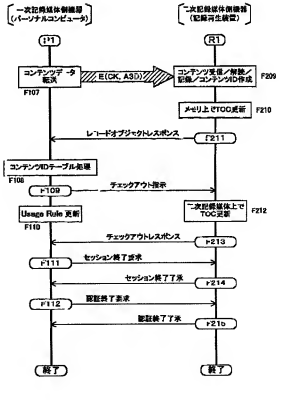
Check In Response Command

オフセット (バイト)	MSB 7	6	5	4	3	2	1	LSB 0
00h	CTS				response : ACCEPTED			
⋮	⋮							
0Ah	Op Code : Check In							
0Bh	result							
0Ch	Subfunction							
0Dh	List ID							
0Eh								
0Fh	object position number							
10h	プリペイド情報							
11h								
12h								
13h								
14h								
15h								
16h								
17h								
18h								

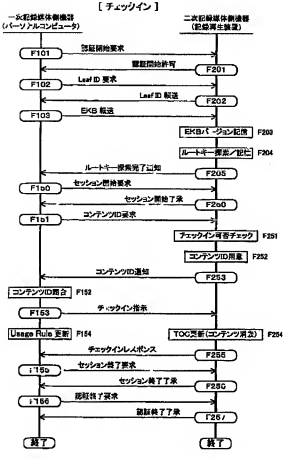
【図26】



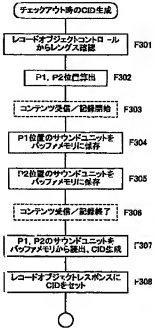
【図27】



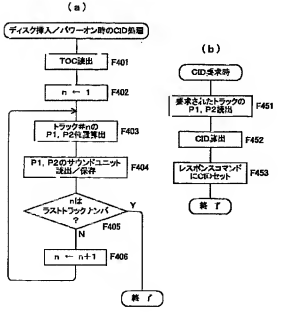
【図28】



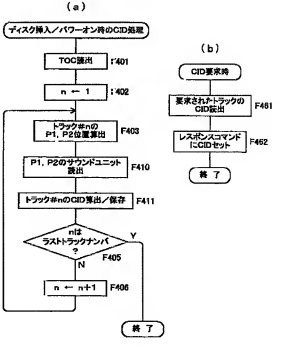
【図31】



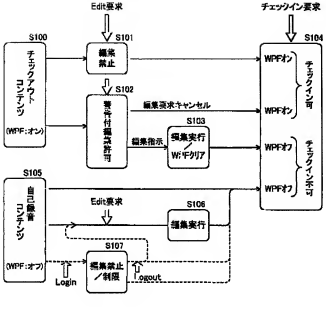
【図32】



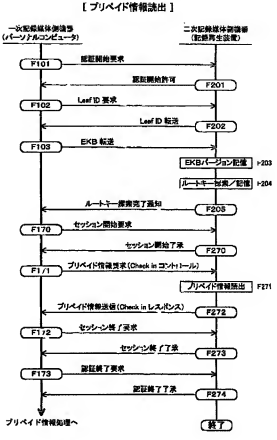
【図33】



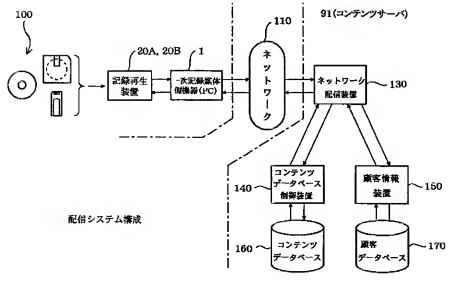
【図34】


Edit要求
チェックイン要求
S100
チェックアウトコンテンツ
(WPF:オン)
S101
編集禁止
S102
警告付編集許可
編集要求キャンセル
S103
編集指示
編集実行
Wドクリア
S104
WPFオン
チェックイン可
WPFオン
WPFオン
チェックイン不可
WPFオン
S105
自己保存コンテンツ
(WPF:オフ)
Edit要求
S106
編集実行
S107
編集禁止／制限
Login
Logout

【図35】


【プリペイド情報読出】
一次記録媒体制御部
(パーソナルコンピュータ)
二次記録媒体制御部
(記録再生装置)
F101
認証開始要求
F201
認証開始許可
F102
Leaf ID 要求
F202
Leaf ID 転送
F103
EKB 転送
EKBバージョン記憶
>203
ルートキー復号／記憶
>204
ルートキー復号完了通知
F203
F170
セッション開始要求
F270
セッション開始了承
F171
プリペイド情報要求(Check in コマンド)
プリペイド情報読出
F271
プリペイド情報送信(Check in レスポンス)
F272
F172
セッション終了要求
F273
セッション終了了承
F173
認証終了要求
F274
認証終了了承
プリペイド情報処理へ
終了

【図36】

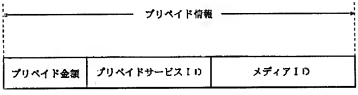

100
20A, 20B
1
110
91(コンテンツサーバ)
記録再生装置
一次記録媒体制御部(PC)
ネットワーク
ネットワーク配信装置
130
コンテンツデータベース制御装置
140
顧客情報装置
150
コンテンツデータベース
160
顧客データベース
170
配信システム構成

【図37】

顧客データベース

	メディアID	残り金額	購入履歴
(K1)	ID1	3700円	・・・・・・・・
(K2)	ID2	100円	・・・・・・・・
(K3)	ID3	1200円	・・・・・・・・
(K4)	ID4	5000円	・・・・・・・・
(K5)	ID5	0円	・・・・・・・・
・・・	・・・	・・・	・・・

【図38】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
H04N 7/173	630	H04L 9/00	601B

(72)発明者 松田 寛美
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 田中 理生
東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B017 AA06 BA07 CA15
5B082 EA11
5C064 BA07 BB02 BC04 BC18 BC22 BC25 BD02 BD07 BD14
5J104 AA07 NA05 PA14